GN-AP01G

AirCruiser G Access Point

User's Manual

www.gigabyte.com.tw
June. 2005
Revision 1.0

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

GIGABYTE declares that GN-AP01G (FCC ID: JCK-GN-AP01G) is limited in CH1~CH11 for 2.4GHz by specified firmware controlled in U.S.A.

Contents

Chapter 1 Introduction 1
Overview 1
Features 1
Package Contents 2
GN-AP01G Rear Panel 2
Status LEDs 3
Chapter 2 QUICK INSTALLATION 4
System Requirements 4
Planning Your Network Environment 4
Hardware Installation 5
Chapter 3 Configuration - Using A Web-Browser 6
Using Web-based Configuration 6
Configuring the Adapter for Access Point Mode Access 7
Chapter 4 Access Point Manager 23
Installing the Access Point Manager 23
Using the Access Point Manager 28
Upgrade Firmware 47
Uninstall AP Manager Utility 49
Chapter 5 Troubleshooting 51
Appendix A: Glossary 52
Appendix B: Specifications 56
Physical Interface 56
Specifications 56
Appendix C: PC Configuration 57
TCP/IP Settings Under Windows 2000 57
TCP/IP Settings under Windows XP 60
Appendix D Warranty 63

Chapter 1 Introduction

Overview

Thank you for purchasing Gigabyte AirCruiser G GN-AP01G Wireless Access Point. The GN-AP01G uses the IEEE 802.11g standard which has 54Mbps bandwidth instead of standard 802.11b or standard Wi-Fi which has 11Mbps bandwidth. The AirCruiser G GN-AP01G Wireless Access Point supports both 802.11b and 802.11g clients.

The GN-AP01G Wireless Access Point is able to connect to either IEEE 802.11g or IEEE802.11b. Providing transmission speeds of up to 54Mbps, the GN-AP01G allows users to share network resources, retrieve emails, download large files, conduct a video conference, and distribute or display digital photos, videos or MP3 files.

Furthermore, the Access Point supports up to 128-bit WEP encryption to safeguard your privacy on-line. GN-AP01G not only enables simple and easy installation and usage, but also provides you useful AP Manager Configuration Utility and Web-based configuration.

Features

- Complies with IEEE 802.11g and 802.11b standards
- Data rates up to 54Mbps
- Supports 64-bit /128-bit WEP encryption, WPA, WPA-PSK, 802.1x
- Supports WDS
- Supports dynamic & static IP address configuration
- Easy web management
- Useful AP Manager Configuration Utility
- Web-based firmware upgrade
- Dynamically adjusts transmission rates for optimum performance

Package Contents

Before installing, please examine the components to ensure that none were damaged during shipping. The package contents of the GN-AP01G shall include:

- ☑ GN-AP01G AirCruiser G Access Point
- ☑ Power Adapter
- ☑ Installation CD containing User's Guide
- ☑ Quick Installation Guide
- ☑ Ethernet Cable

If there are any missing or damaged parts, please contact your local distributor or dealer immediately. If a replacement unit is needed, return the device with the original packing material, otherwise the warranty will be void.

GN-AP01G Rear Panel

1. Power Socket

2. Ethernet LAN Port
   10/100Mbps LAN connection with auto-sensing and MDI/MDIX

3. Antenna
   Removable high gain 2.4GHz dipole-type

Status LEDs

LED's

Please see the table below for a description of the LEDs:

Label	Activity	Description
Power	On (Green) Off	Power is supplied to the Access Point Power is NOT supplied to the Access Point
WLAN	On (Green) Blink	Wireless link is connected Data is being transmitted wirelessly
LAN	On (Green) Blink	LAN port has detected a link with a 10/100 Mbps device Data is being transmitted

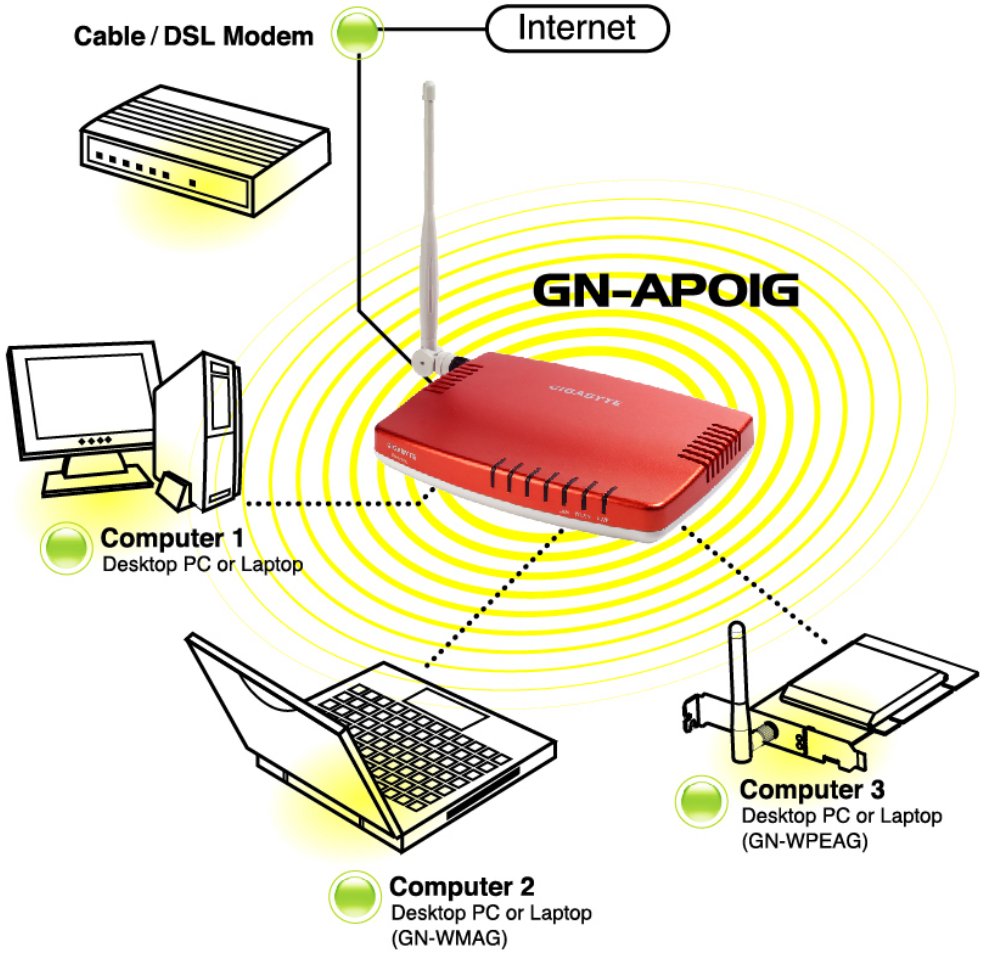
Chapter 2 QUICK INSTALLATION

System Requirements

Suggested Specifications for Wireless LAN Access Point installation:

- A PC, Notebook or Macintosh Computer with installed 802.11b/g wireless LAN adapter
- An Ethernet router or hub
- Ethernet patch cable

Planning Your Network Environment



You can build your network environment as the picture above. After you set up the access point, you can surf the internet by wireless from your PC, PDA and Notebook which built-in wireless module.

Hardware Installation

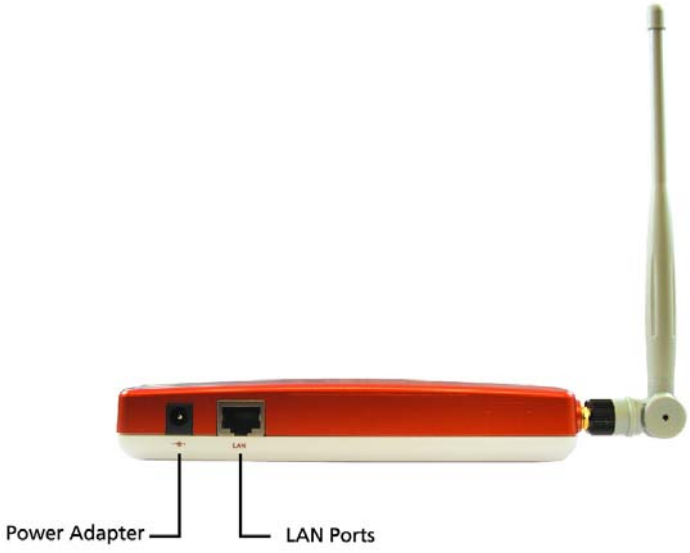
Follow the steps below when installing your Access Point(s).

Before you begin, please keep the following in mind when placing your Access Point(s).

- ✓ Select a suitable location to install the Access Point. Assure that the location is **away** from any interfering radio signals from devices such as microwave ovens, garage door openers, vacuum cleaning devices, etc. Please also operate the Access Point in a cool dry place, away from direct sunlight.

- ✓ Position the Access Point appropriately. Signal strength is greatly dependent on your well placed Access Point. Generally, a centralized area with 360° clear line of sight is the best location with the antenna in a high position to allow optimal propagation of the signal. **The location of the Access Point greatly influences the signal reception.**

Installing the Access Point



Step 1 Turn off all the hardware devices in your network.

Step 2 Connect the Ethernet cable of your router/hub to the LAN port of the Access Point.

Step 3 Plug the power adapter cord into the router's power jack and then plug the power adapter into a power outlet.

Step 4 Turn on all the hardware devices in your network. After verifying all the connections, proceed to **Appendix C: PC Configuration**

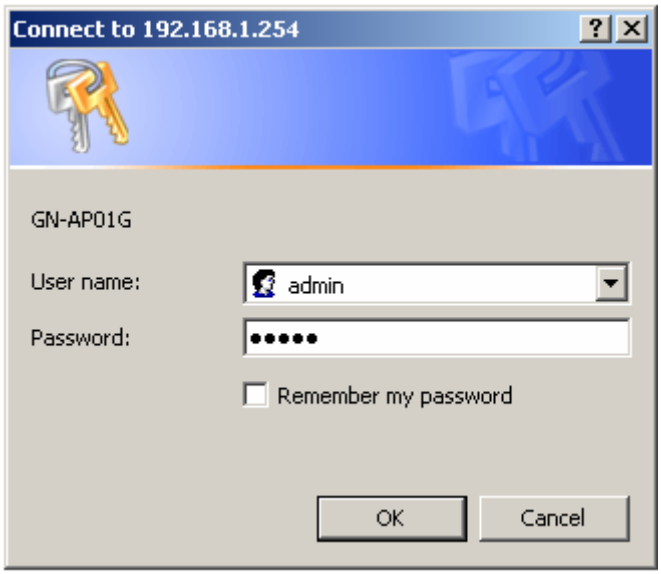
Chapter 3 Configuration - Using A Web-Browser

This section explains the web-based configuration method of setting up the Access Point. Any Internet Explorer 5.0 or above or Netscape Communicator 6.0 or above may be used to administer the GN-AP01G AirCruiser G Access Point.

Using Web-based Configuration

Open the web-browser of your choice, and enter the local IP address of the GN-AP01G AirCruiser G Access Point into the address line of browser. (The factory default local IP is 192.168.1.1) and press **Enter**.

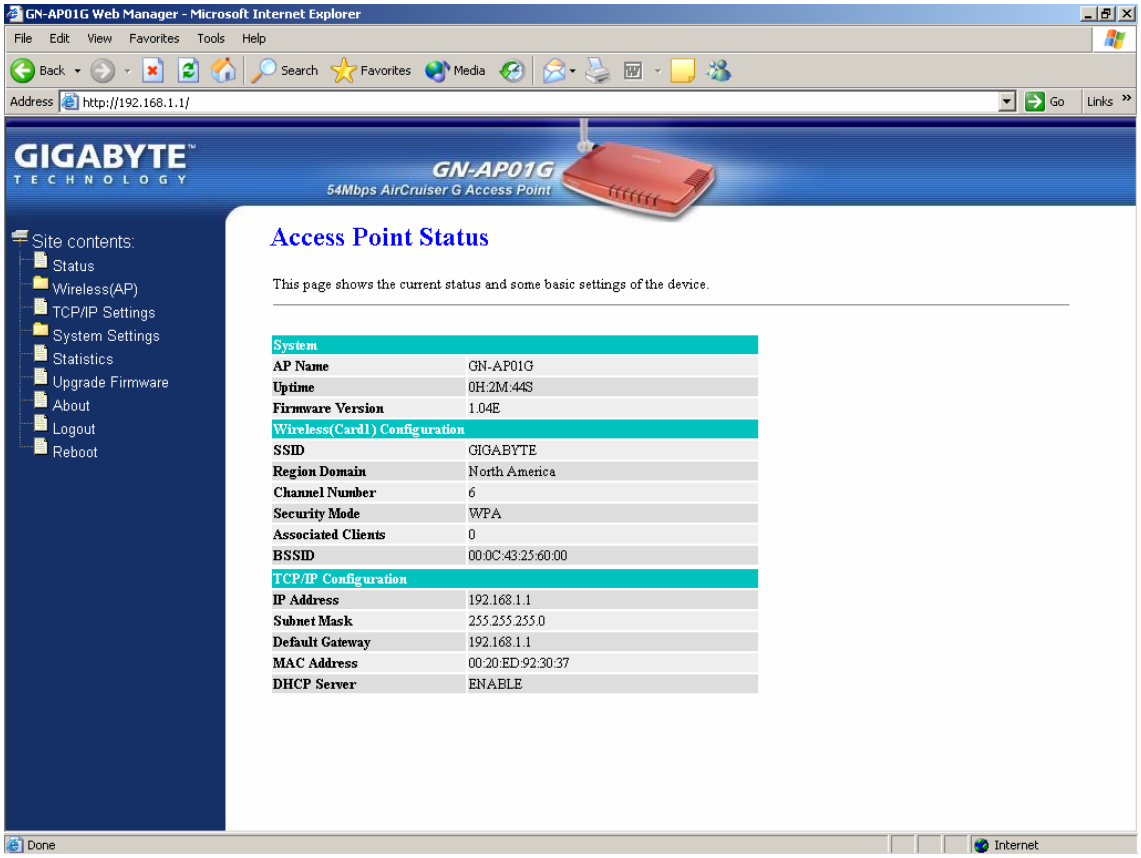
The screen shown as below will appear. In lowercase letters, enter the default user name and password, **admin**, in the User Name and *Password* fields. Click the **OK** button.



Configuring the Adapter for Access Point Mode Access

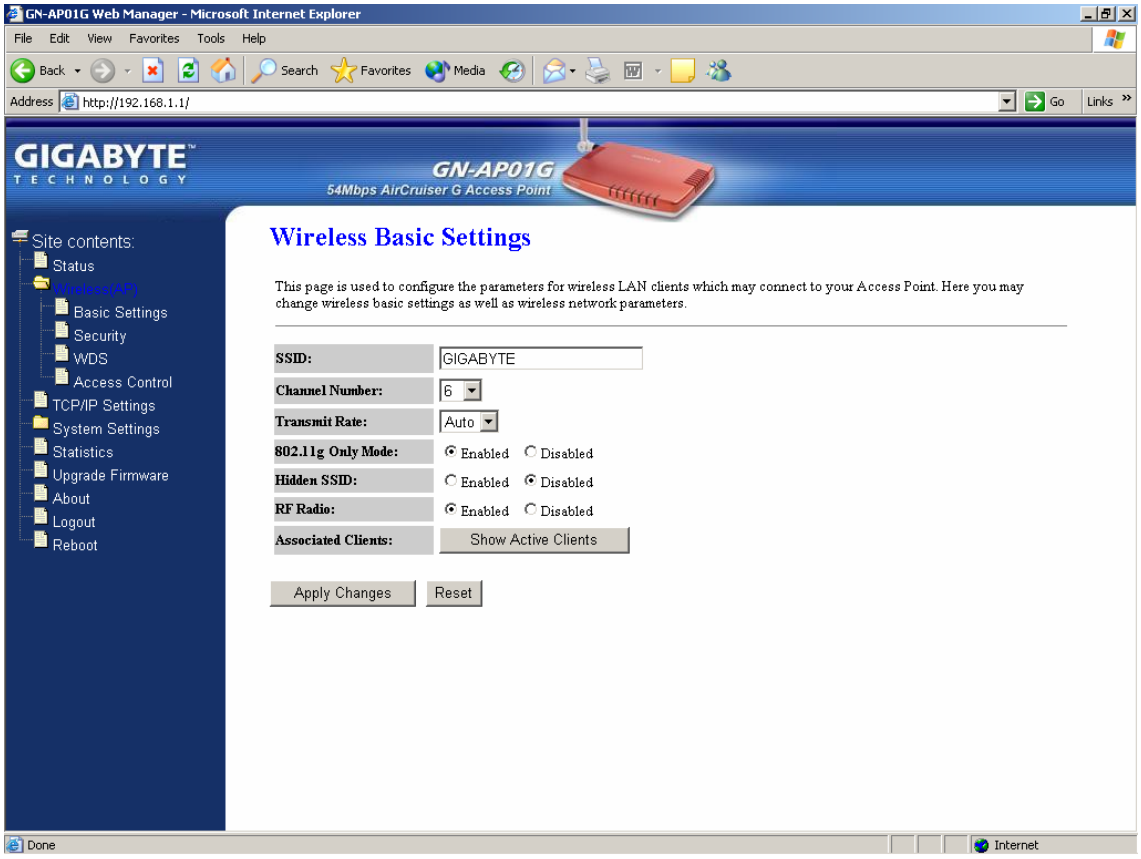
Status

You can use this status screen to view the Access Point's system information, current connection status and configuration.



Wireless Basic Settings

The Access Point will automatically detect and display your wireless settings. Changes of these settings will influence your wireless connection and performance.



SSID

ESSID (or SSID as it is usually referred to) is the network name of the Access Point in the wireless network. You should set the same SSID name for all your wireless-equipped devices to allow dynamic clients to easily roam among them. The SSID name can be up to 32 characters in length and is case sensitive (i.e. upper case letters **"A~Z"** and lower case **"a~z"** are unique).

Channel Number

Please choose the channel for best performance. Normally, no change is needed.

Transmit Rate

Select the desired data rate. The range is from 1 to 54Mbps and the default rate is set to "Auto".

802.11g Only Mode

Enabled -- No Wireless-B clients will be allowed on the network.

Disabled – Both Wireless-G and Wireless-B clients will be allowed on the network. (Default setting)

Hidden ESSID

This setting enables you to hide ESSID name, which is needed by clients in order to connect to the Access Point. The default value is **"Disable"**. In this setting, ***all users are able to read your AP's SSID name.***

RF Radio

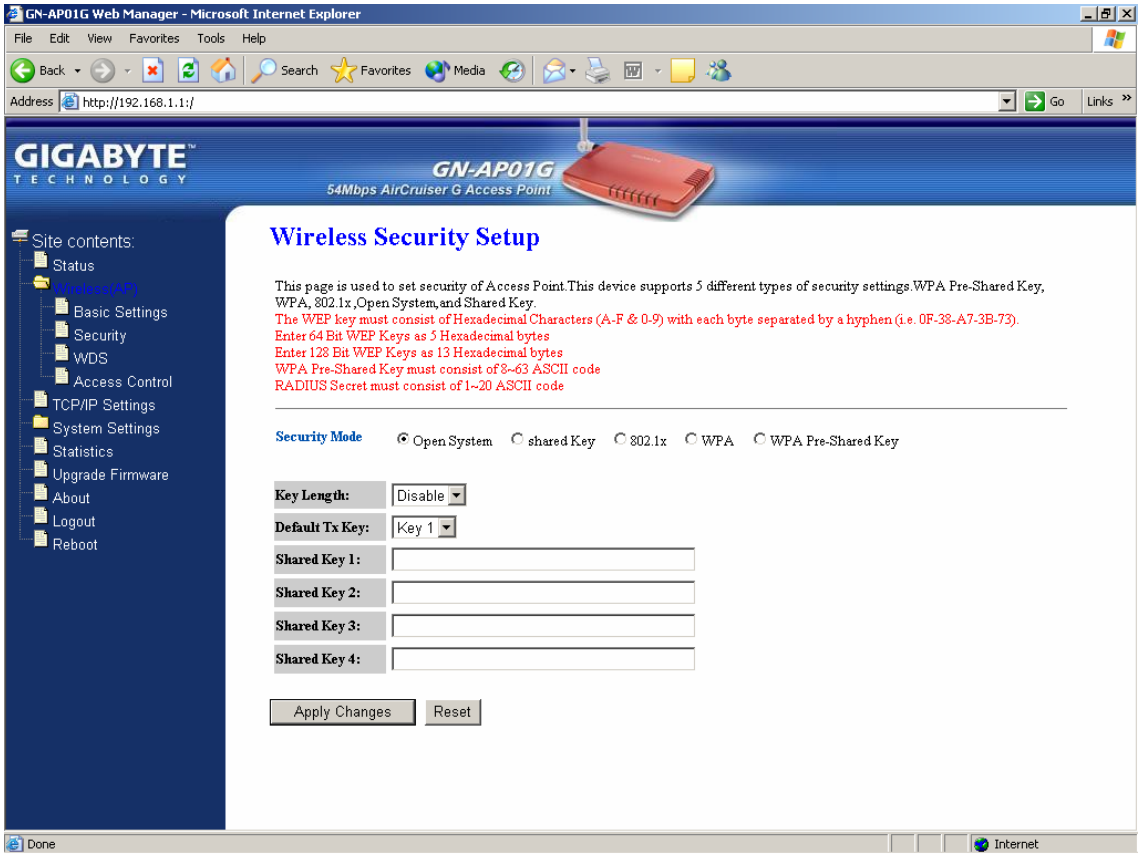
Enable or disable the RF Radio function.

Associated Clients

Click **"Show Active Clients"** button to obtain the connecting users' information.

Wireless Security Setting

Use this feature to set up the security types for the Access Point. Five security types are available: Open System, Shared Key, 802.1x, WPA and WPA Pre-Shared Key.



*** Open system**

Allows any device to connect to the network, assuming the device's SSID matches the access point's SSID.

*** Shared Key**

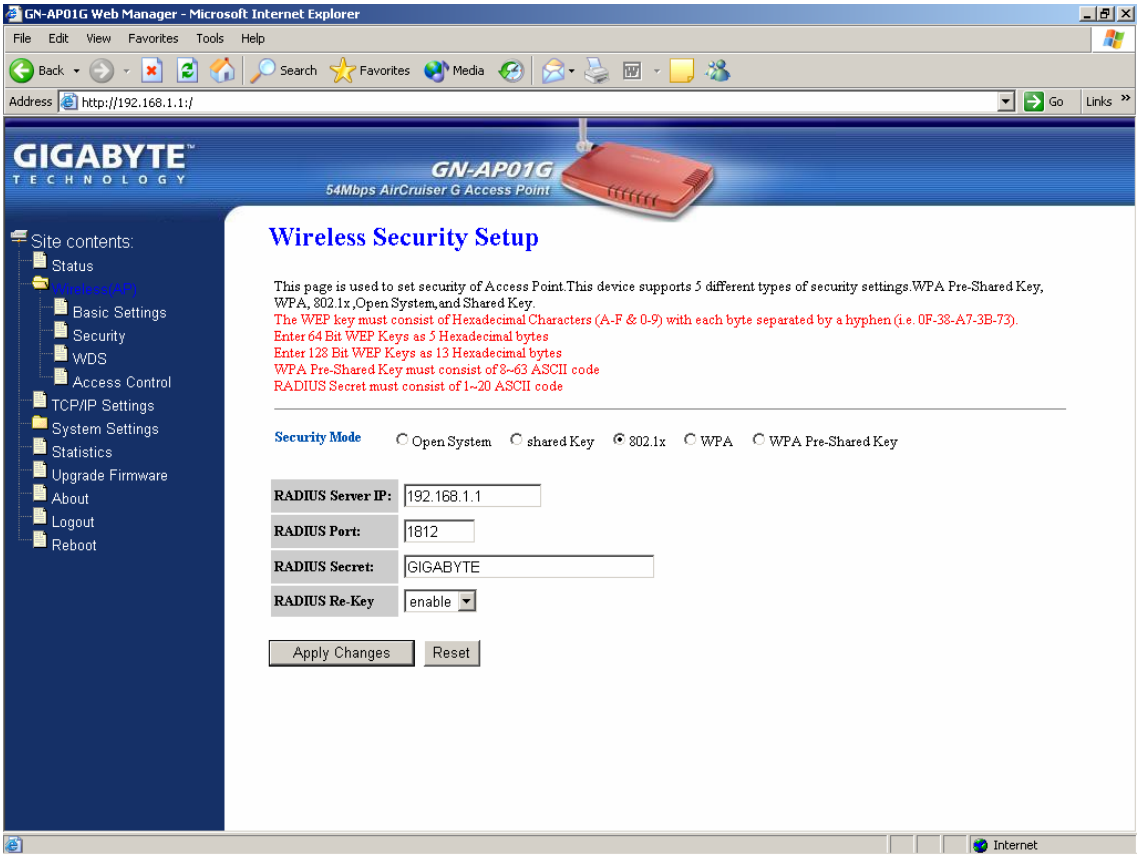
Only those computers that have the correct authentication key can join the network.

Key Length choice

Disable - No encryption will be applied.

64-bit - enter 5 hexadecimal digits.

128-bit - enter 13 hexadecimal digits.

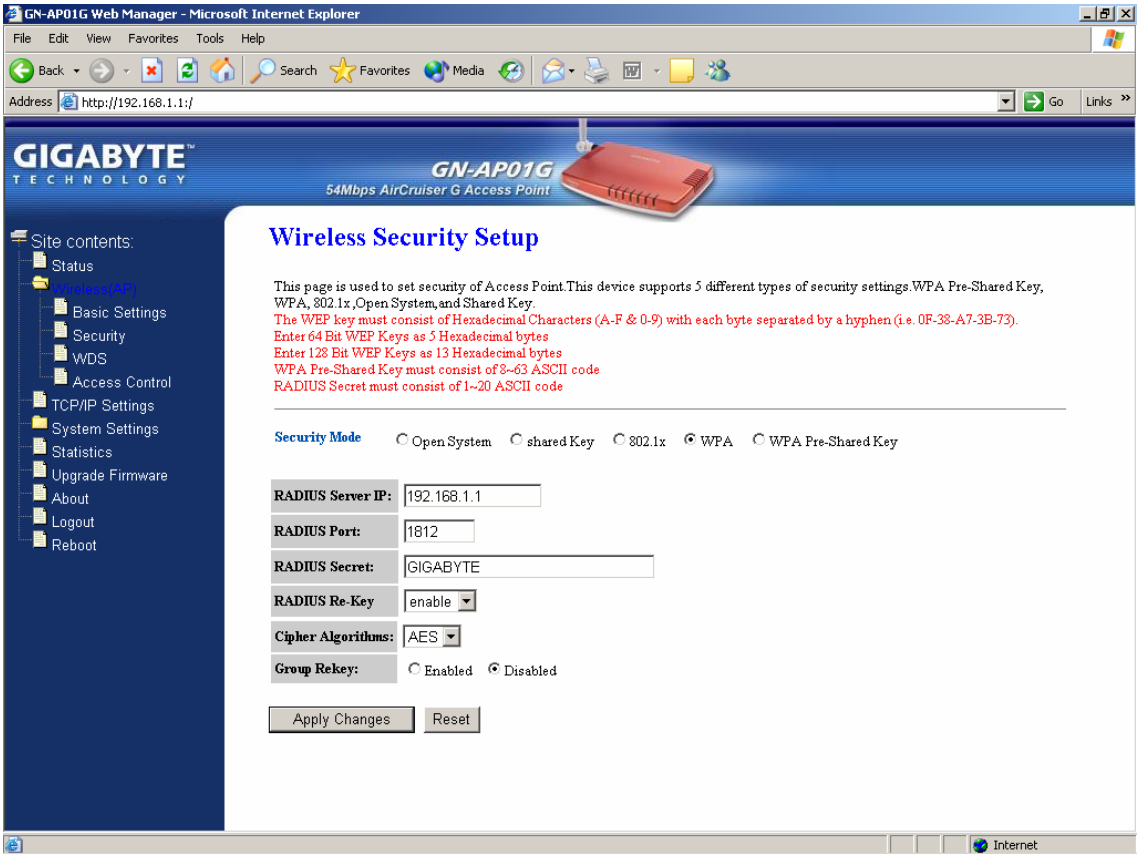


*** 802.1x**

802.1x is IEEE standard for EAP encapsulation over wired or wireless Ethernet. 802.1x uses three terms that you need to know. The user or client that wants to be authenticated is called a supplicant. The actual server doing the authentication, typically a RADIUS server, is called the authentication server. And the device in between, such as a wireless access point, is called the authenticator. One of the key points of 802.1x is that the authenticator can be simple and dumb - all of the brains have to be in the supplicant and the authentication server. This makes 802.1x ideal for wireless access points, which are typically small and have little memory and processing power.

RADIUD Server IP – Assign an IP address for the RADIUS Server.
RADIUS Port – Enter a value within the range 1~65536 for port.
RADIUS Secret – Enter a password up to 32 ASCII characters (uppercase “A~Z”, lowercase “a~z”, or numeric “0~9”) in length.
RADIUS Re-key – Lets you enable or disable the RADIUS Re-Key function.

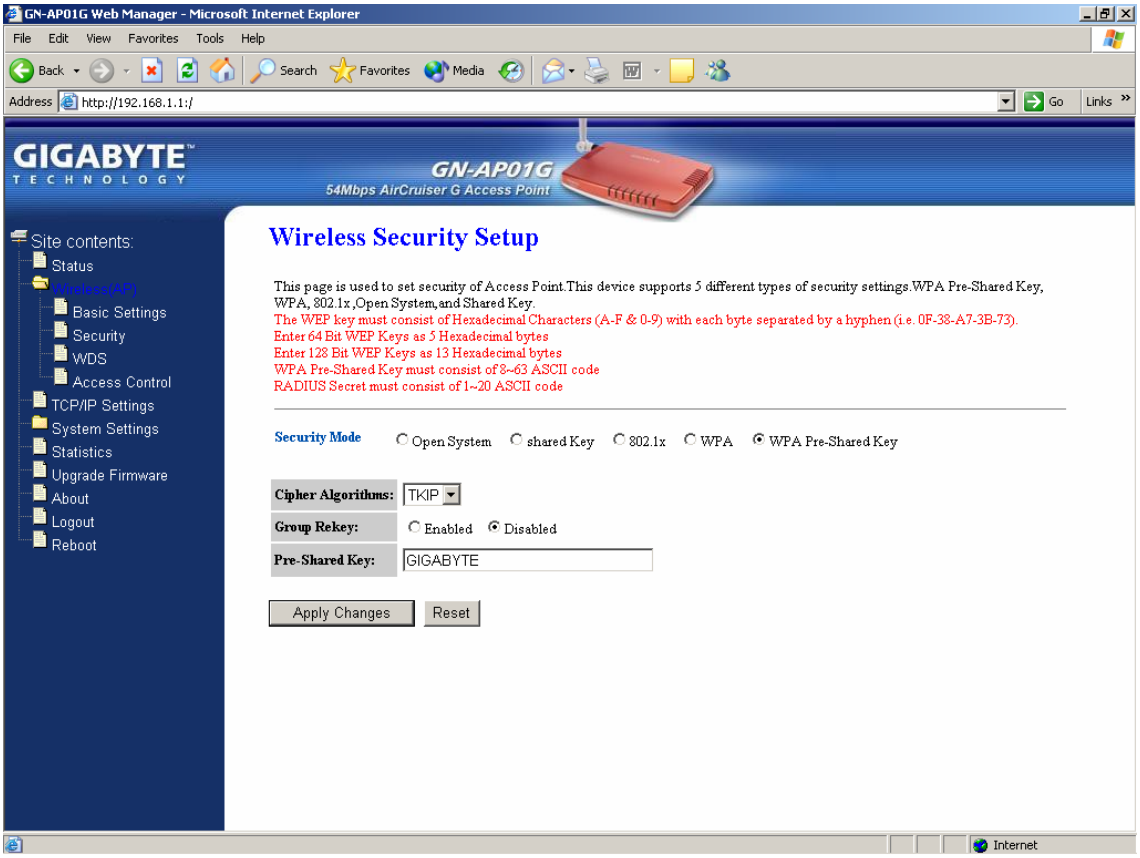
GN-AP01G AirCruiser G Access Point



* WPA (Wi-Fi Protected Access)

If you have used Wi-Fi for a while, you may be familiar with 802.1x Authentication Protocol, which allows users to authenticate the wireless network via RADIUS server. The 802.1x Authentication Protocol is an option in standard Wi-Fi but a must for WPA.

RADIUD Server IP – Assign an IP address for the RADIUS Server.
RADIUS Port – Enter a value within the range 1~65536 for port.
RADIUS Secret – Enter a password up to 32 ASCII characters (uppercase “A~Z”, lowercase “a~z”, or numeric “0~9”) in length.
RADIUS Re-key – Lets you enable or disable the RADIUS Re-Key function.
Cipher Algorithms – Two options you can choose: TKIP and AES settings.
Group Re-key - Lets you enable or disable the RADIUS Re-Key function.



* WPA Pre-Shared Key

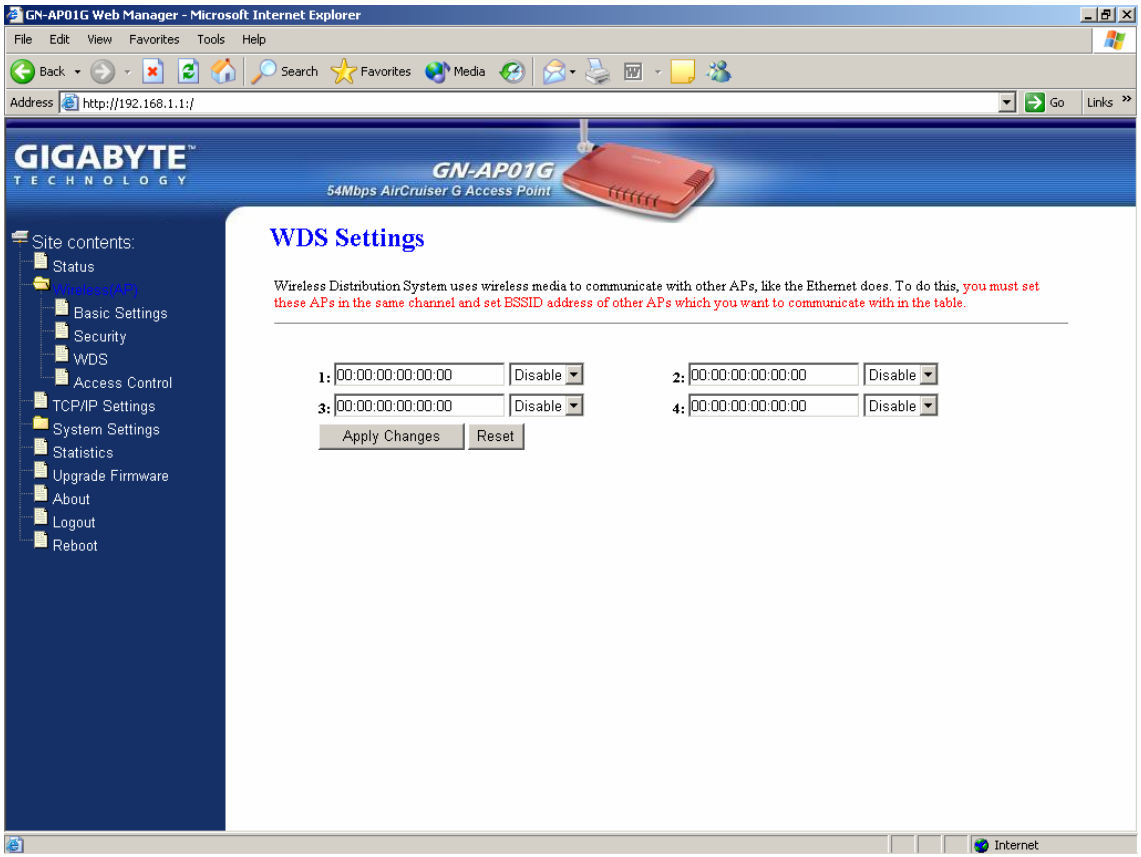
Traditional WEP had an inconvenient method to change encrypted keys. Even when you changed the encrypted keys; you still can not select all APs and wireless LAN adapter while you are changing encrypted keys.

The manual re-keying which is necessary with WEP is a tedious manual process and is completely impractical for large organizations. After all, the instant you re-key an access point, none of the clients will be able to access it until they too are re-keyed. But with WPA, the re-keying of global encryption keys is all that is necessary. In the case of unicast traffic, the encryption key is changed after every frame using Temporary Key Integrity Protocol (TKIP). This protocol allows key changes to occur on a frame-by-frame basis and to be automatically synchronized between the access point and the wireless client. Global re-keying works by advertising the new keys to the wireless clients.

Cipher Algorithms – Two options you can choose: TKIP and AES settings.
Group Re-key - Two options: Enabled or Disabled.
Pre-Shared key - Enter a password up to 63 ASCII characters (uppercase “A~Z”, lowercase “a~z”, or numeric “0~9”) in length.

WDS Settings

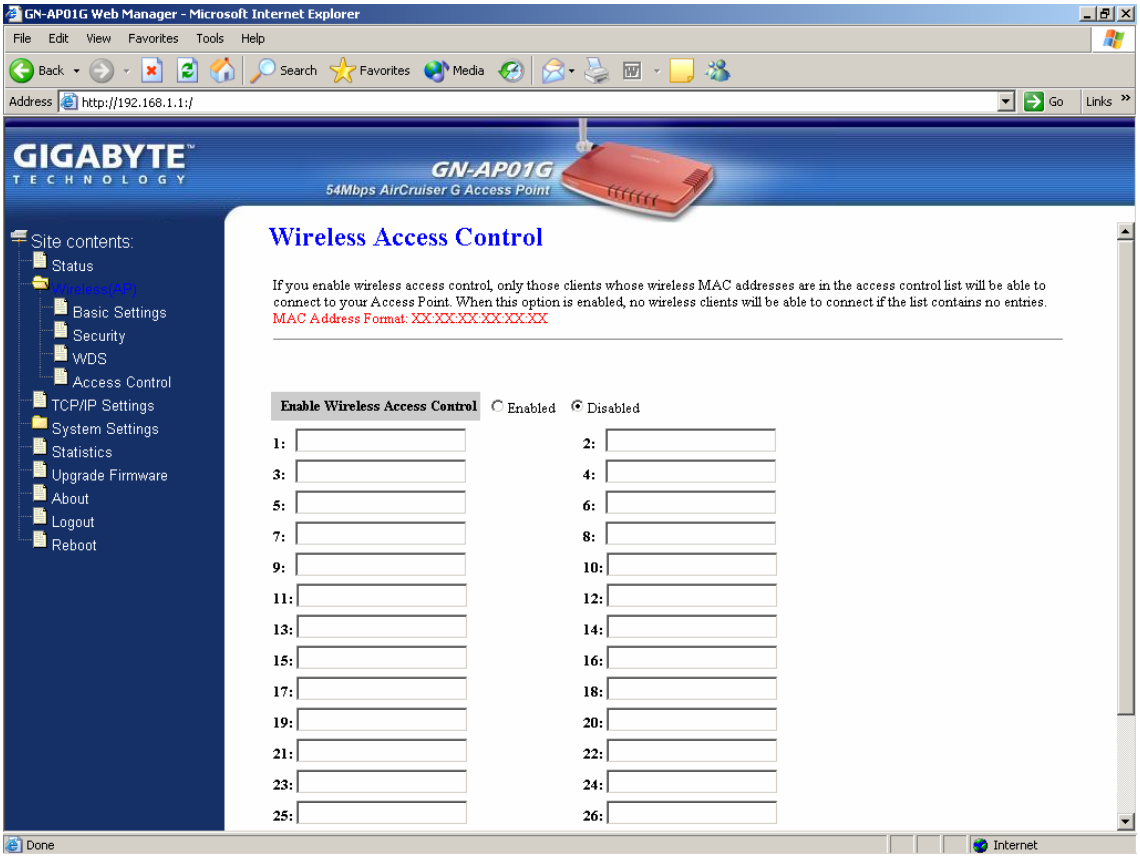
The WDS function allows several of the access points to compose a wide Wireless LAN network. Please note all APs must be set to use the same channel and the SSID of all participating APs must also be the same.



WDS technologies between AP manufacturers vary widely, so you may not be able to establish WDS between APs from different manufacturers.

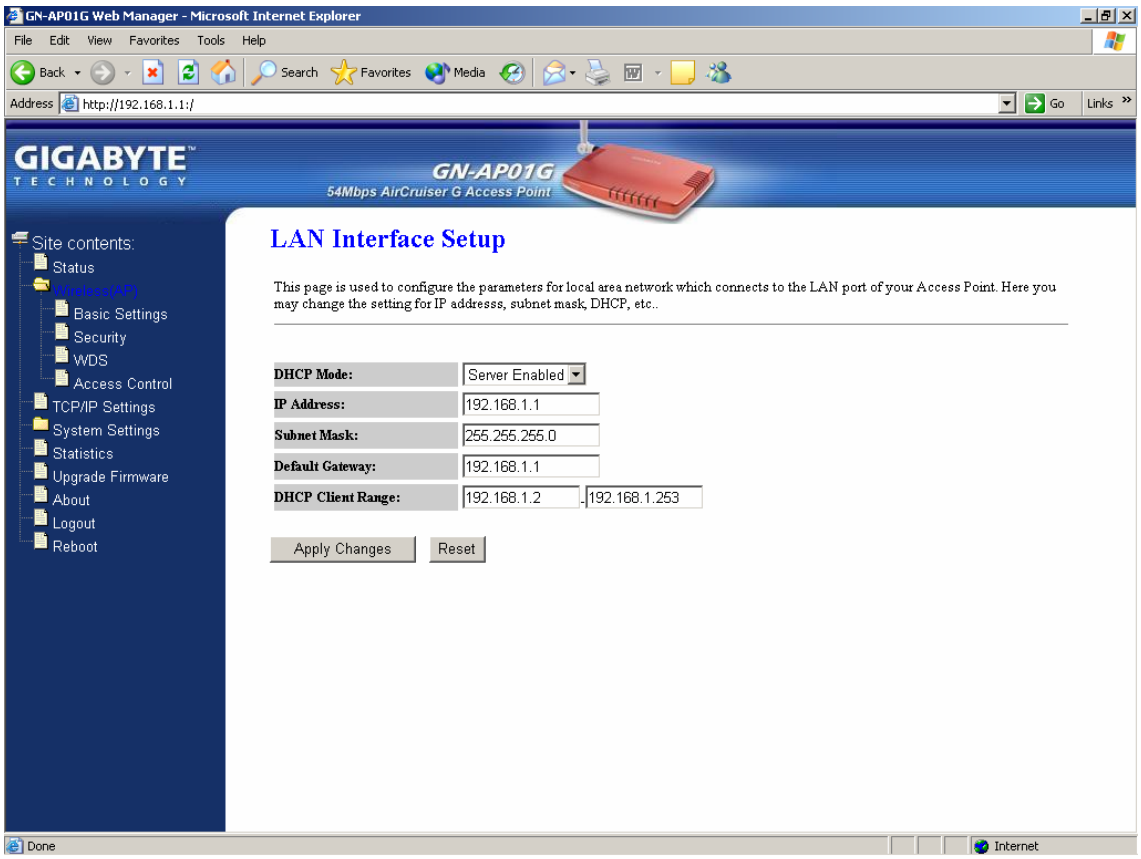
Wireless Access Control

You may specify users based on their MAC addresses that are authorized to connect to the AP. Only computers listed in the table can connect to AP when this function is enabled.



TCP/IP Settings

You may set up IP parameters for APs through TCP/IP setting screen.



DHCP Mode

Three (3) options are available: “Disabled”, “Client Enabled” , “Server Enabled”. The default value is “Server Enabled”.

If you want to obtain IP addresses from a DHCP server, select **“Client Enabled”**. To use an AP as a DHCP server and assign a dynamic IP address automatically on the network, select **“Server Enabled”**.

IP Address

Assign an IP address to the AP with this option. The default IP address is 192.168.1.1. Please make sure the assigned IP address is exclusive for the AP.

Subnet Mask

Assign a Subnet Mask for an AP. The default Subnet Mask is 255.255.255.0.

Default Gateway

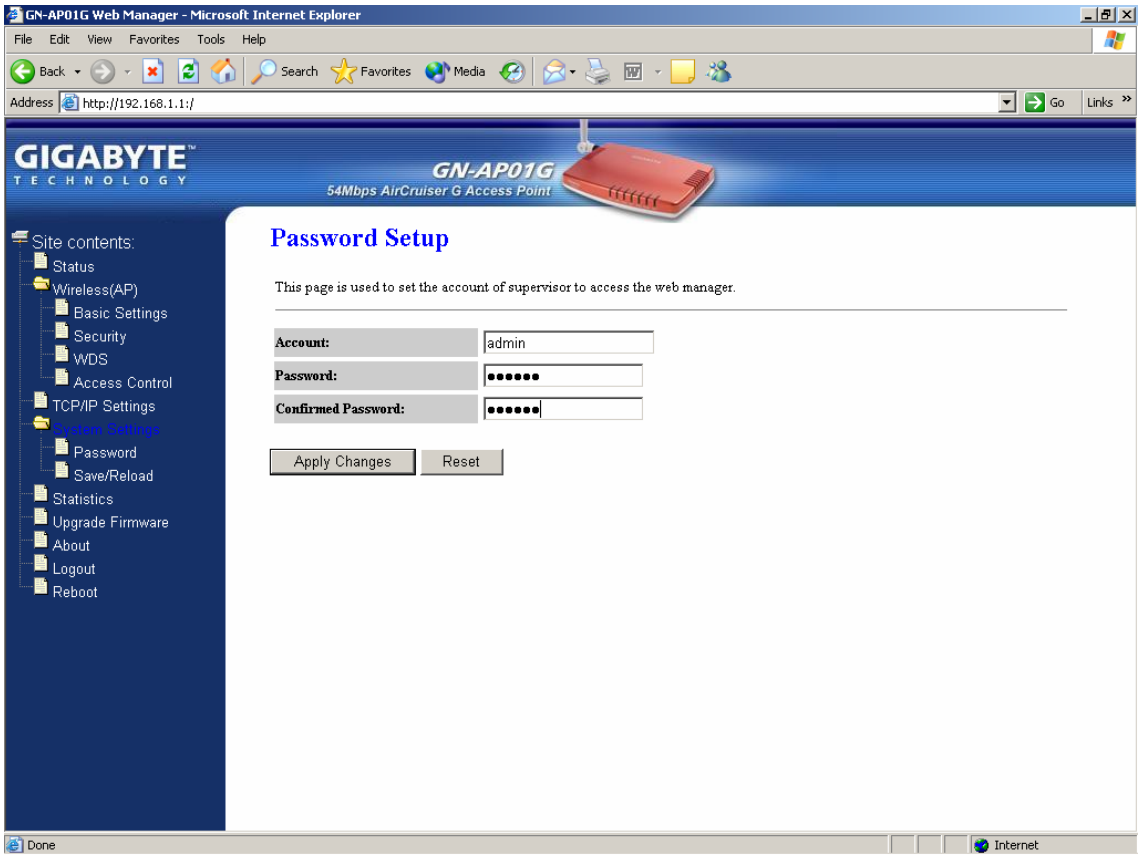
Enter the IP address for the default router. The default gateway is 192.168.1.1.

DHCP Client Range

When “Server Enabled” is selected, please enter the range of your IP addresses.

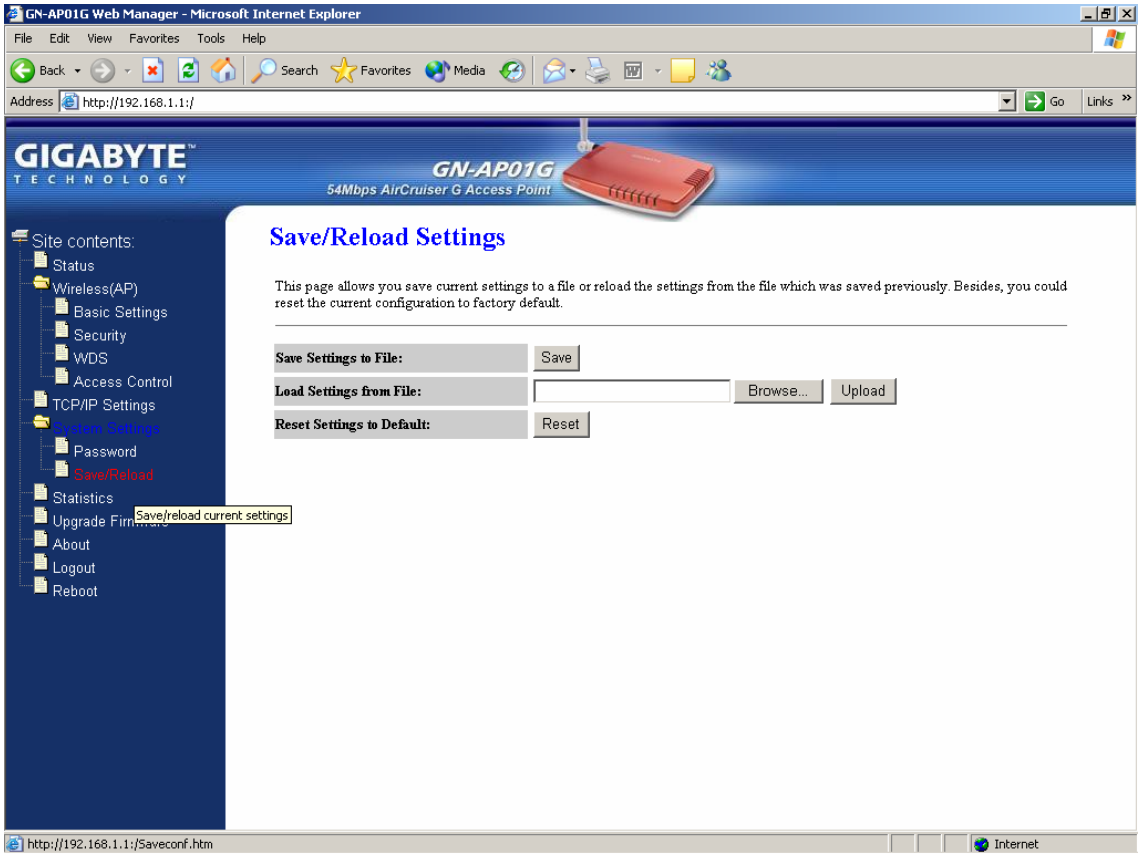
System Settings-Password Setup

Here you can set up administrator's user name and password to restrict administrative access to the AP. Key in a password and confirm, then press Apply Changes. Note, if you leave the password fields blank, password feature is disabled.



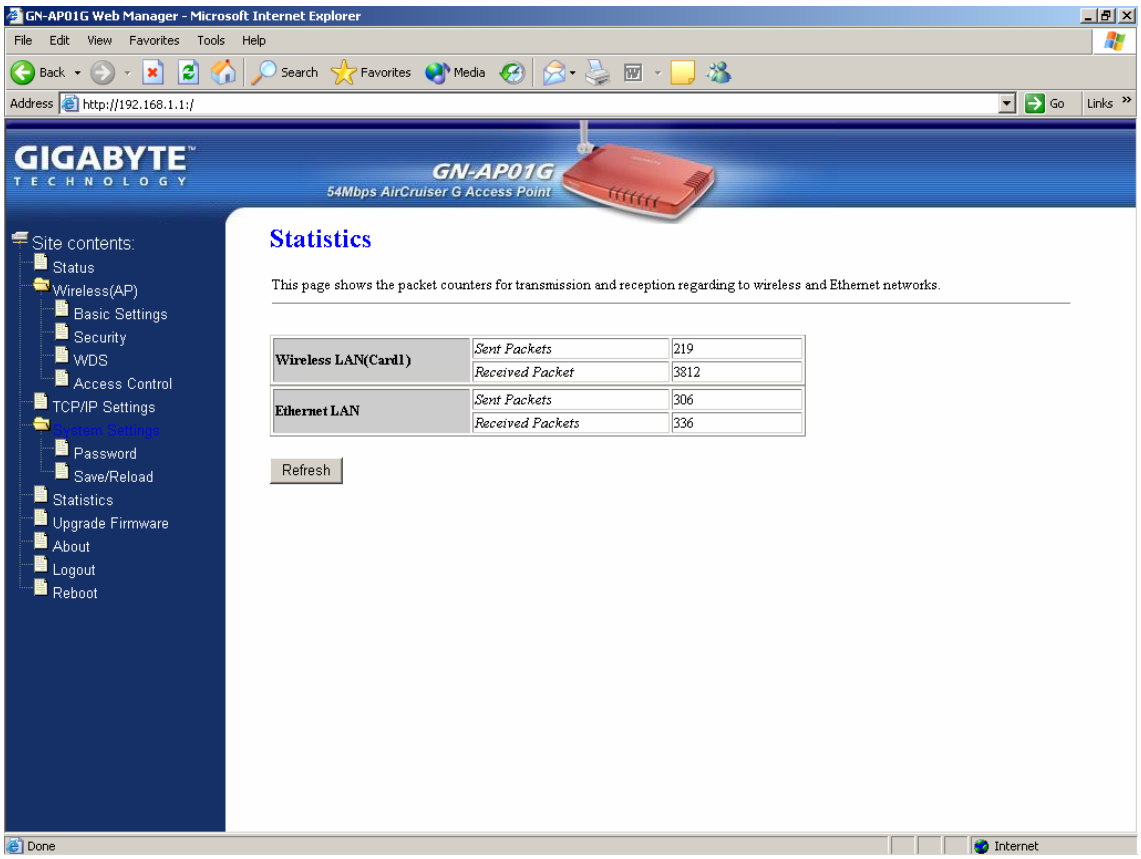
System Settings-Save/Reload Settings

You may save the current configuration as a file for restoring configuration in the future. You may press “Reset” to restore to factory default.



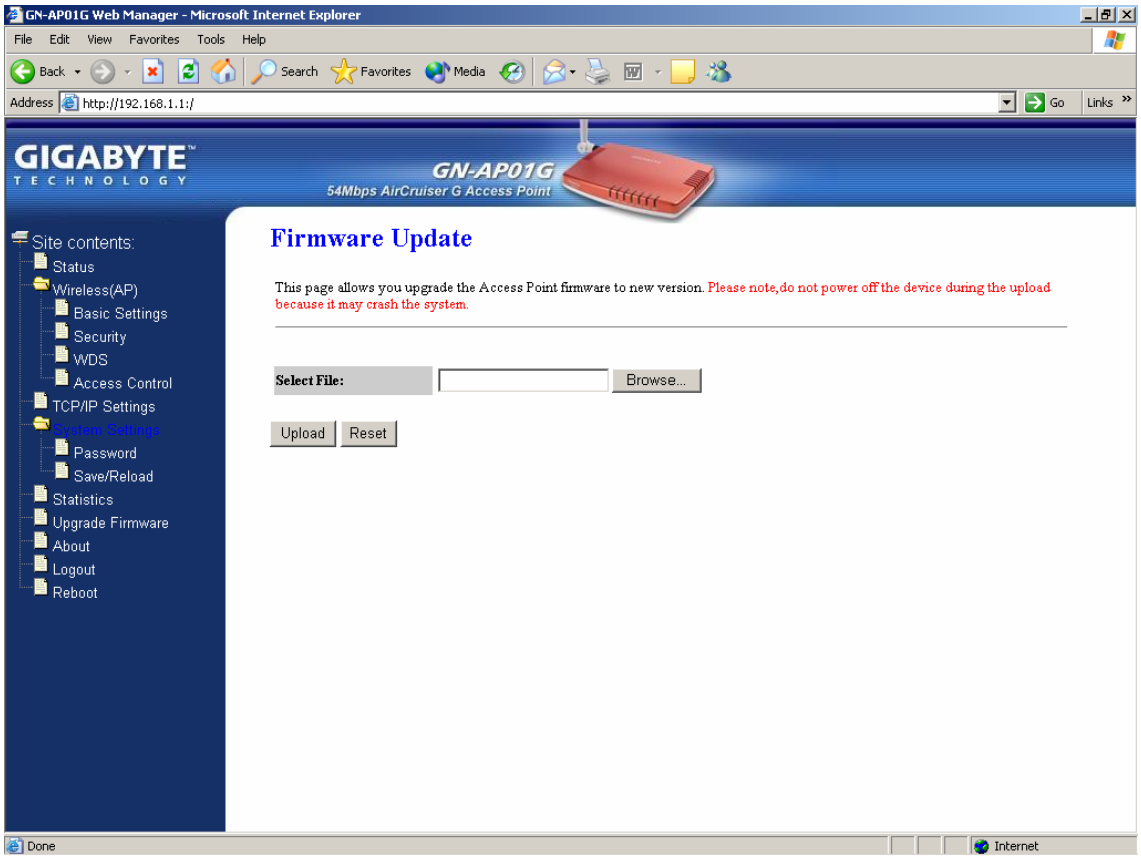
Statistics

Statistics shows you the packet flow status on the wireless LAN and Ethernet.



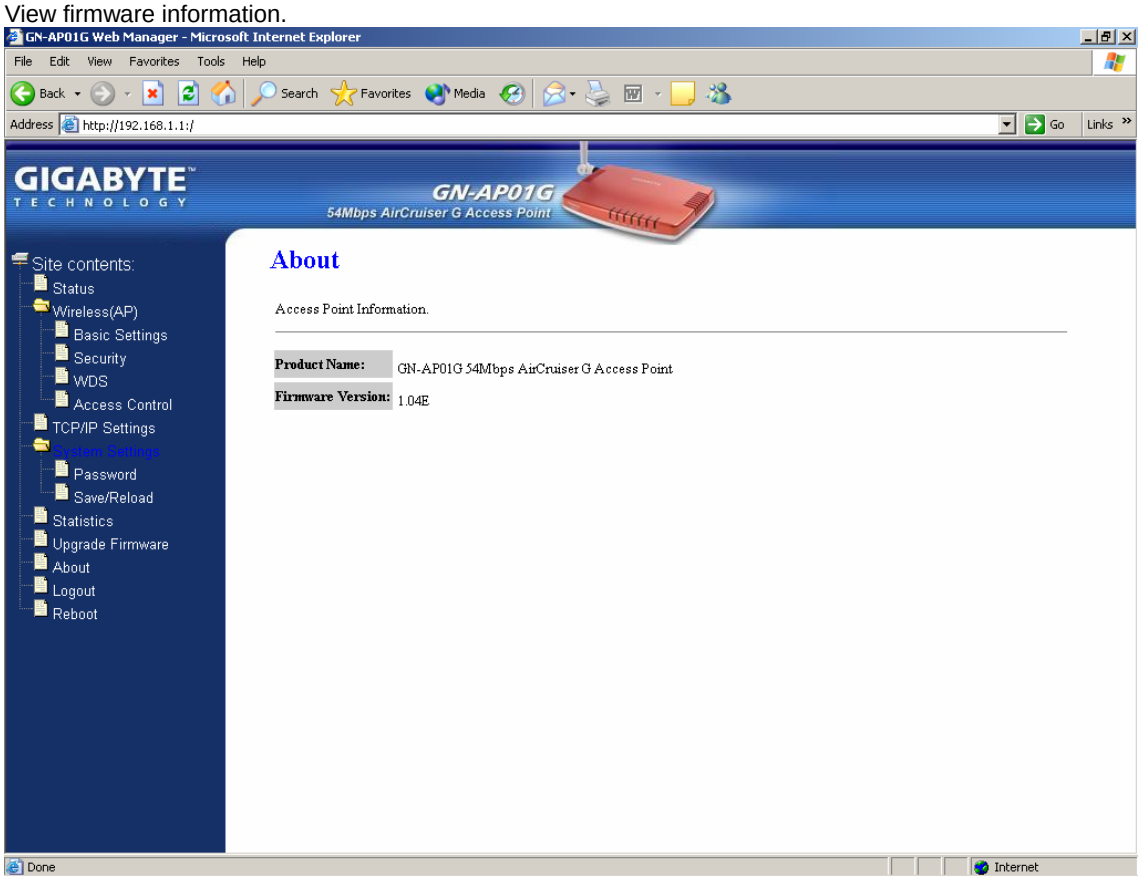
Upgrade Firmware

Upgrade the firmware with the latest firmware version available for download from the GIGABYTE website.



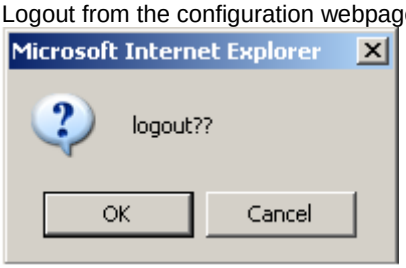
About

View firmware information.



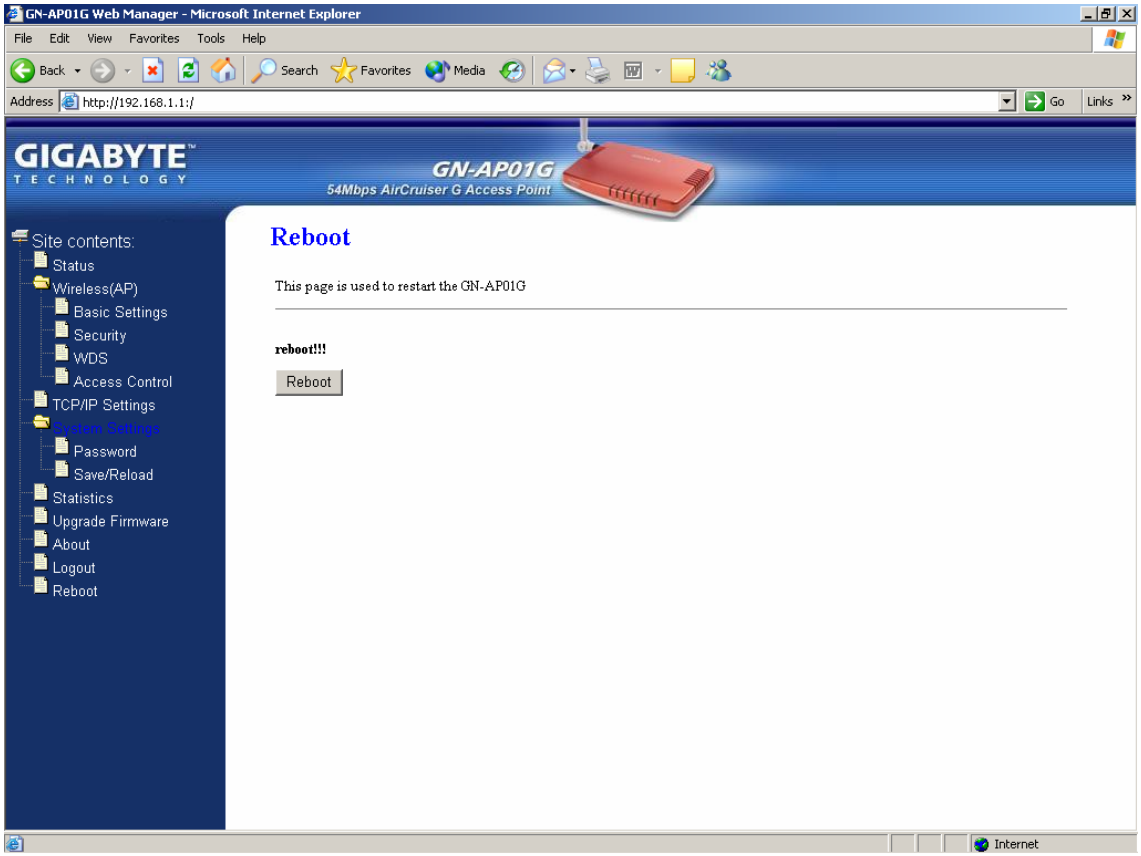
Logout

Logout from the configuration webpage when you finish.



Reboot

Reboot the GN-AP01G. The system may take up to 30 seconds to save your settings, please allow the system to reboot itself.



Chapter 4 Access Point Manager

The Gigabyte Access Point Manager is used to configure Gigabyte Access Points.

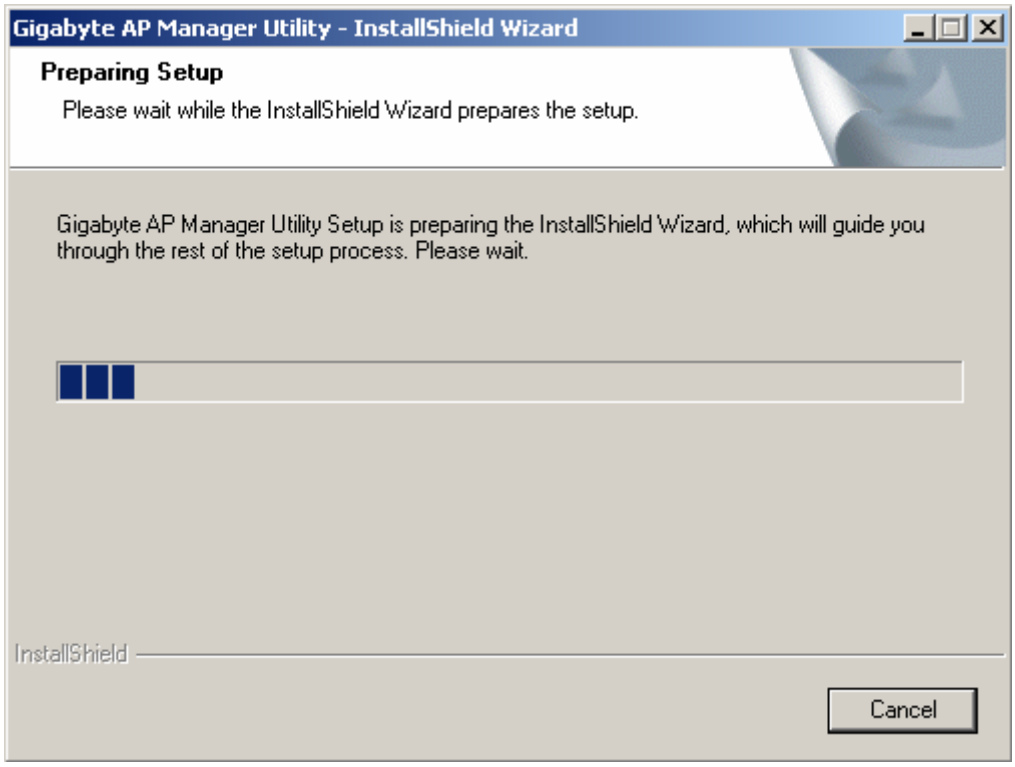
Note: *The performance of wired link is better than wireless link for each Access Point running AP Manager. Use the wired link to manage the Access Point is recommended.*

Installing the Access Point Manager

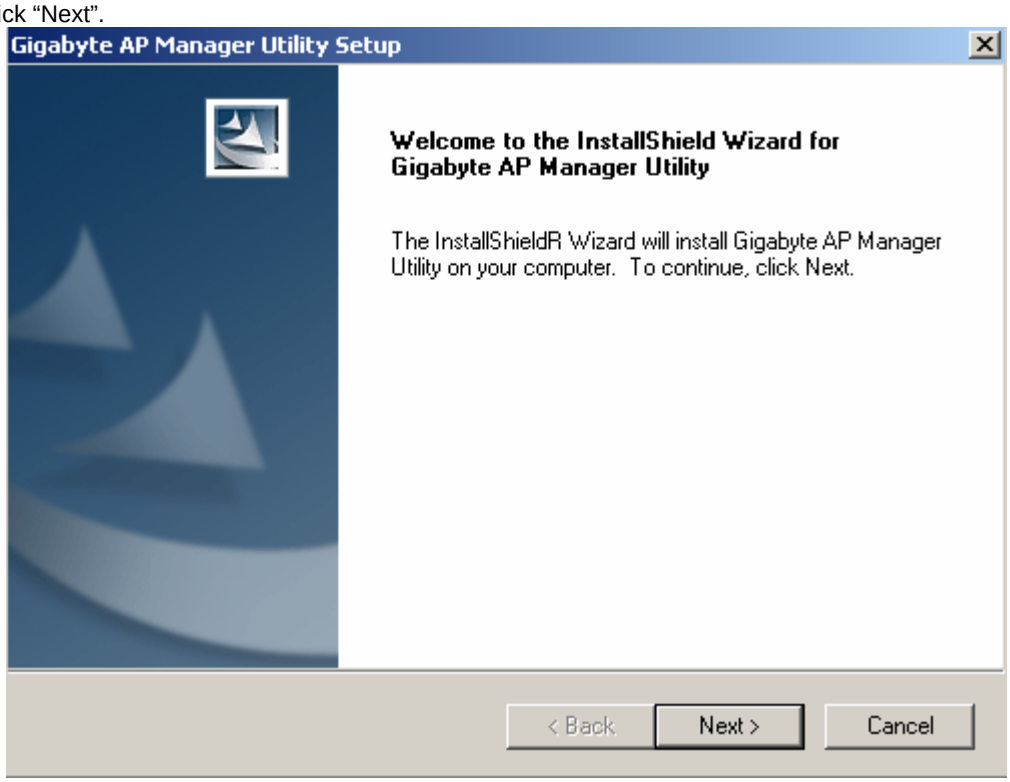
Please do the following steps to install the Gigabyte AP Manager.

Step1. Insert the installation CD and click Install **Gigabyte AP Manager** on the CD auto run screen.

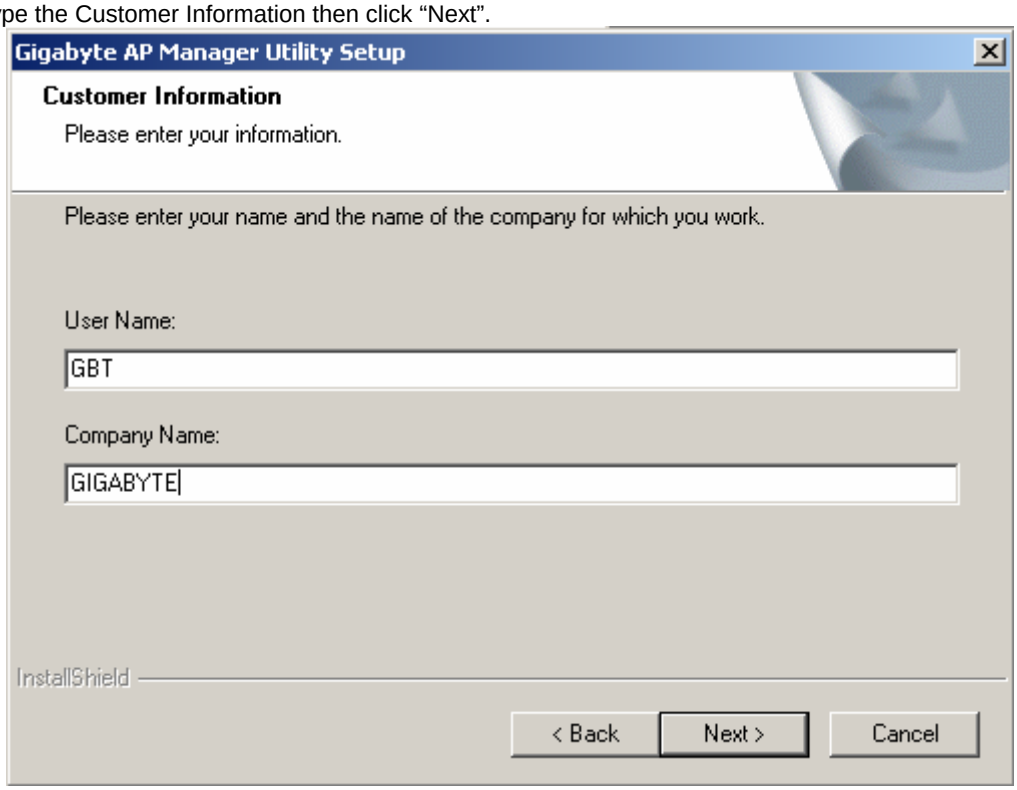
Step2. Please wait a while!!


Gigabyte AP Manager Utility - InstallShield Wizard
Preparing Setup
Please wait while the InstallShield Wizard prepares the setup.
Gigabyte AP Manager Utility Setup is preparing the InstallShield Wizard, which will guide you through the rest of the setup process. Please wait.
InstallShield
Cancel

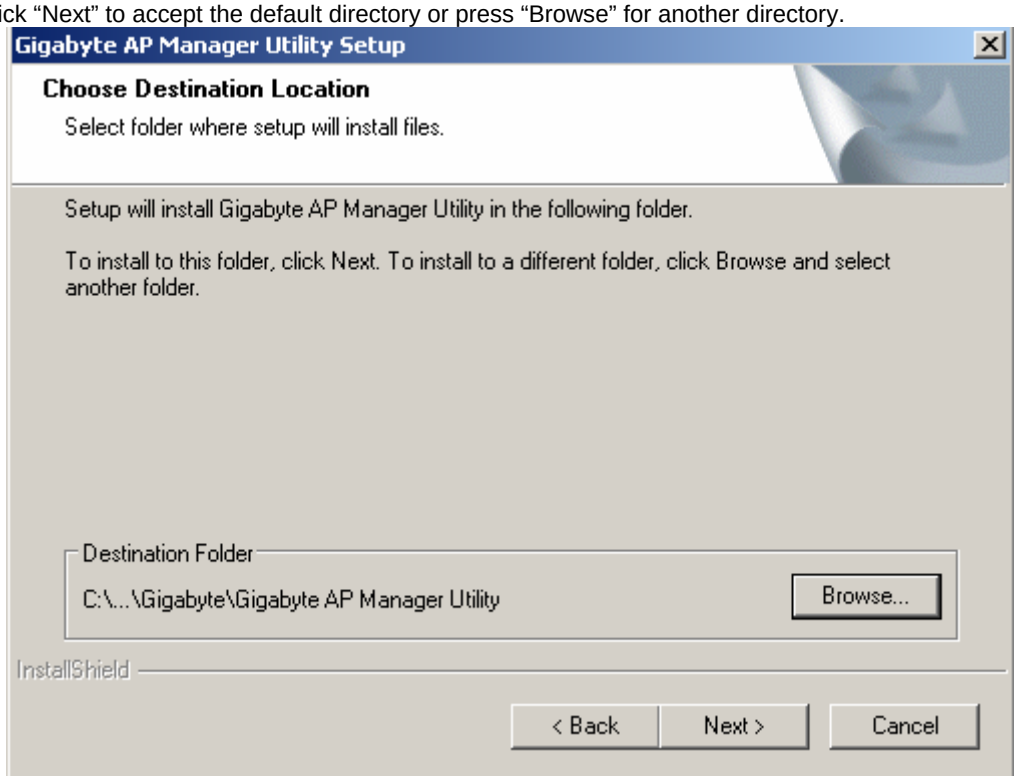
Step3. Click “Next”.


Gigabyte AP Manager Utility Setup
Welcome to the InstallShield Wizard for Gigabyte AP Manager Utility
The InstallShieldR Wizard will install Gigabyte AP Manager Utility on your computer. To continue, click Next.
< Back
Next >
Cancel

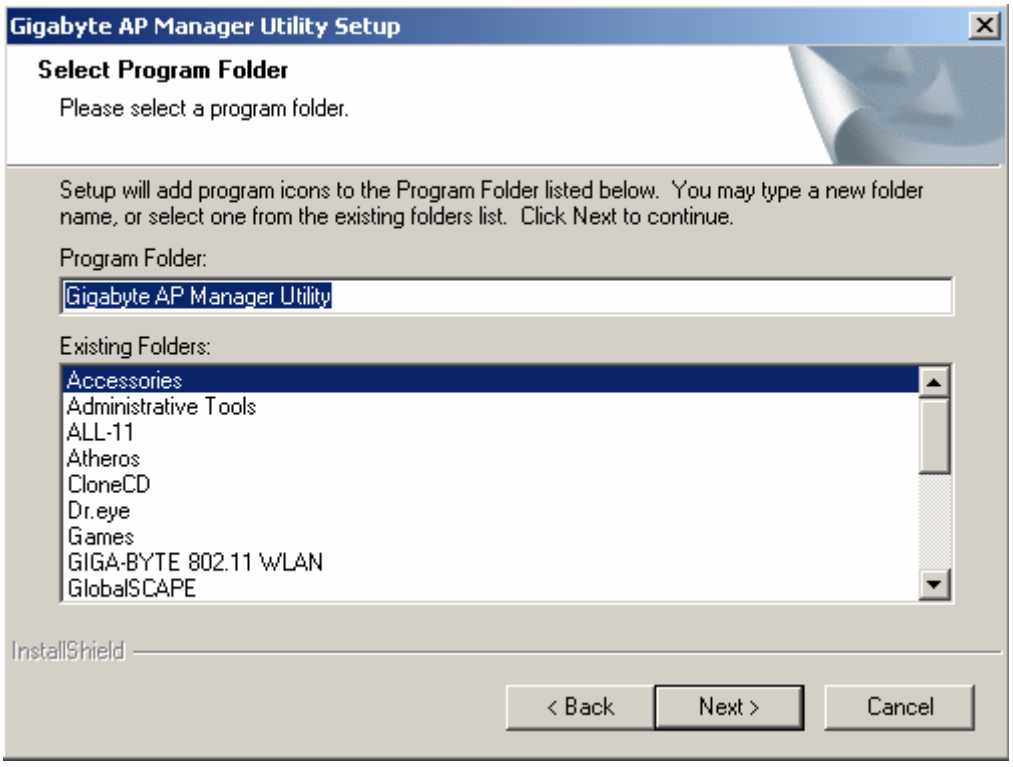
Step4. Type the Customer Information then click “Next”.



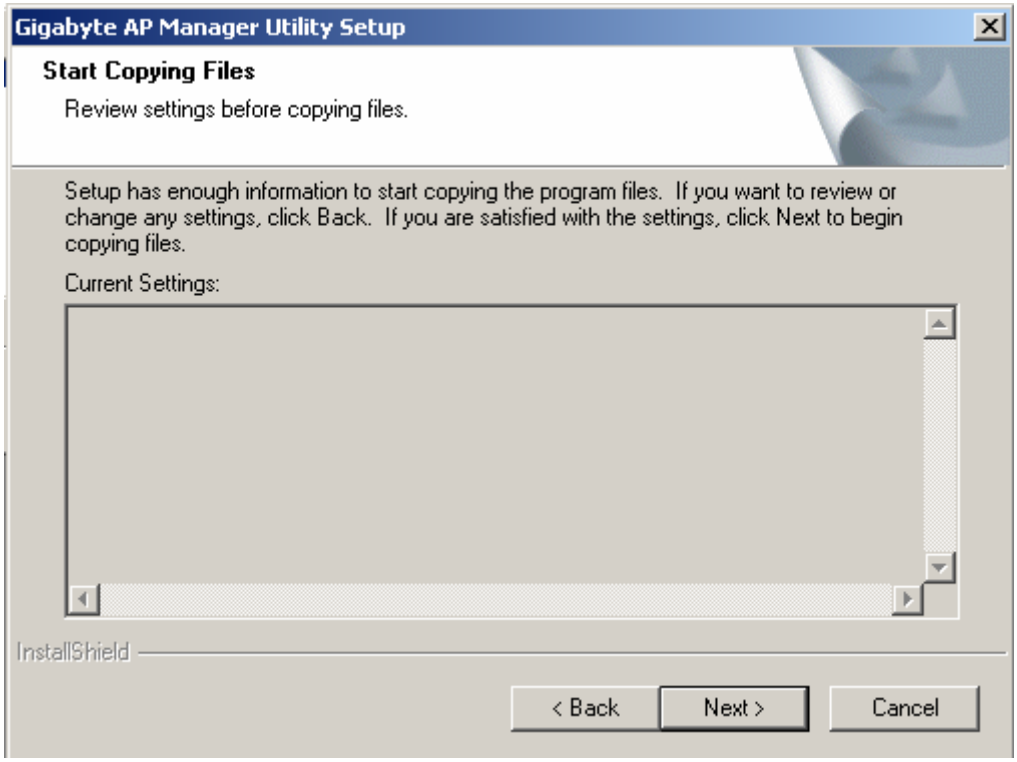
Step5. Click “Next” to accept the default directory or press “Browse” for another directory.


Gigabyte AP Manager Utility Setup
Choose Destination Location
Select folder where setup will install files.
Setup will install Gigabyte AP Manager Utility in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\...\Gigabyte\Gigabyte AP Manager Utility
Browse...
InstallShield
< Back
Next >
Cancel

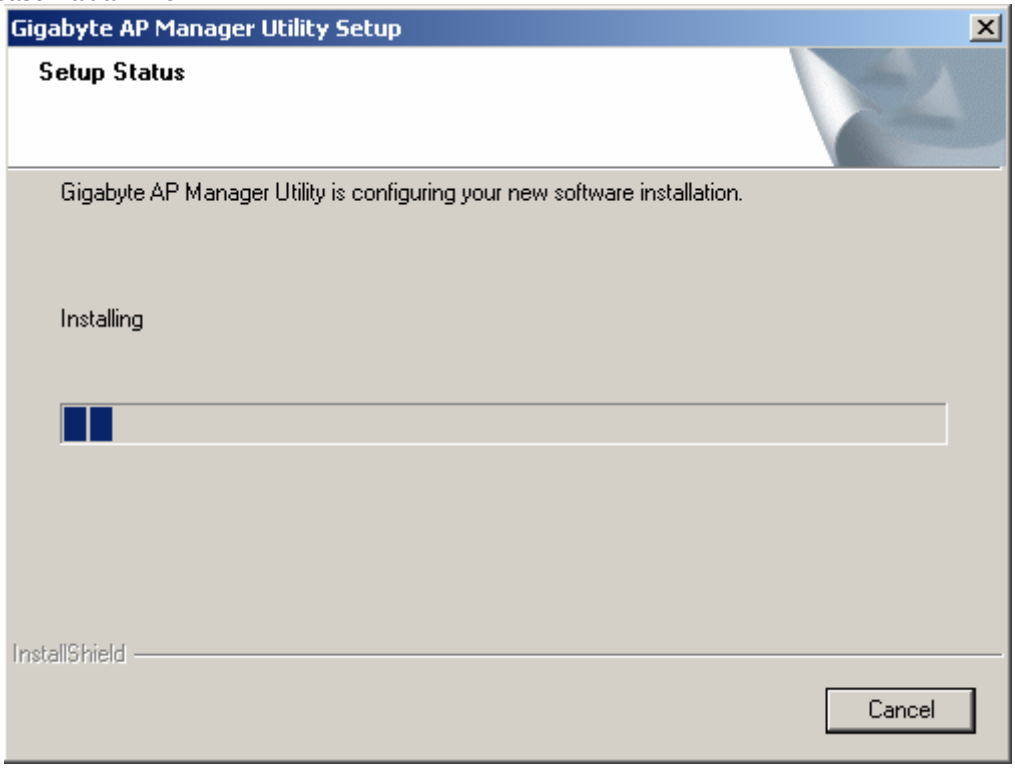
Step6. Click “Next”.



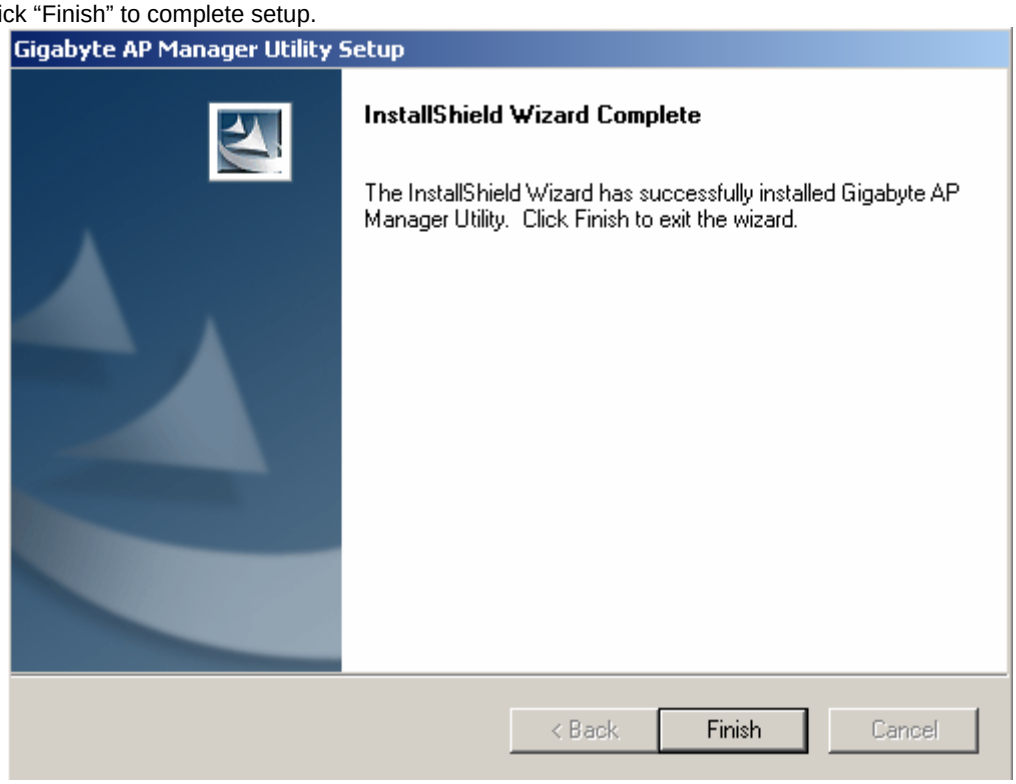
Step7. Click “Next”.


Gigabyte AP Manager Utility Setup
Start Copying Files
Review settings before copying files.
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
InstallShield
< Back
Next >
Cancel

Step8. Please wait a while.



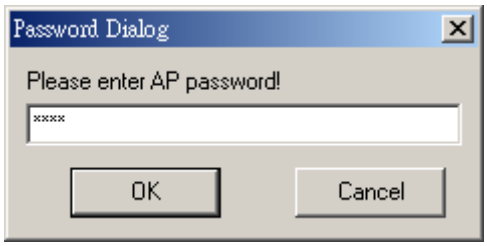
Step9. Click “Finish” to complete setup.


Gigabyte AP Manager Utility Setup
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed Gigabyte AP Manager Utility. Click Finish to exit the wizard.
< Back
Finish
Cancel

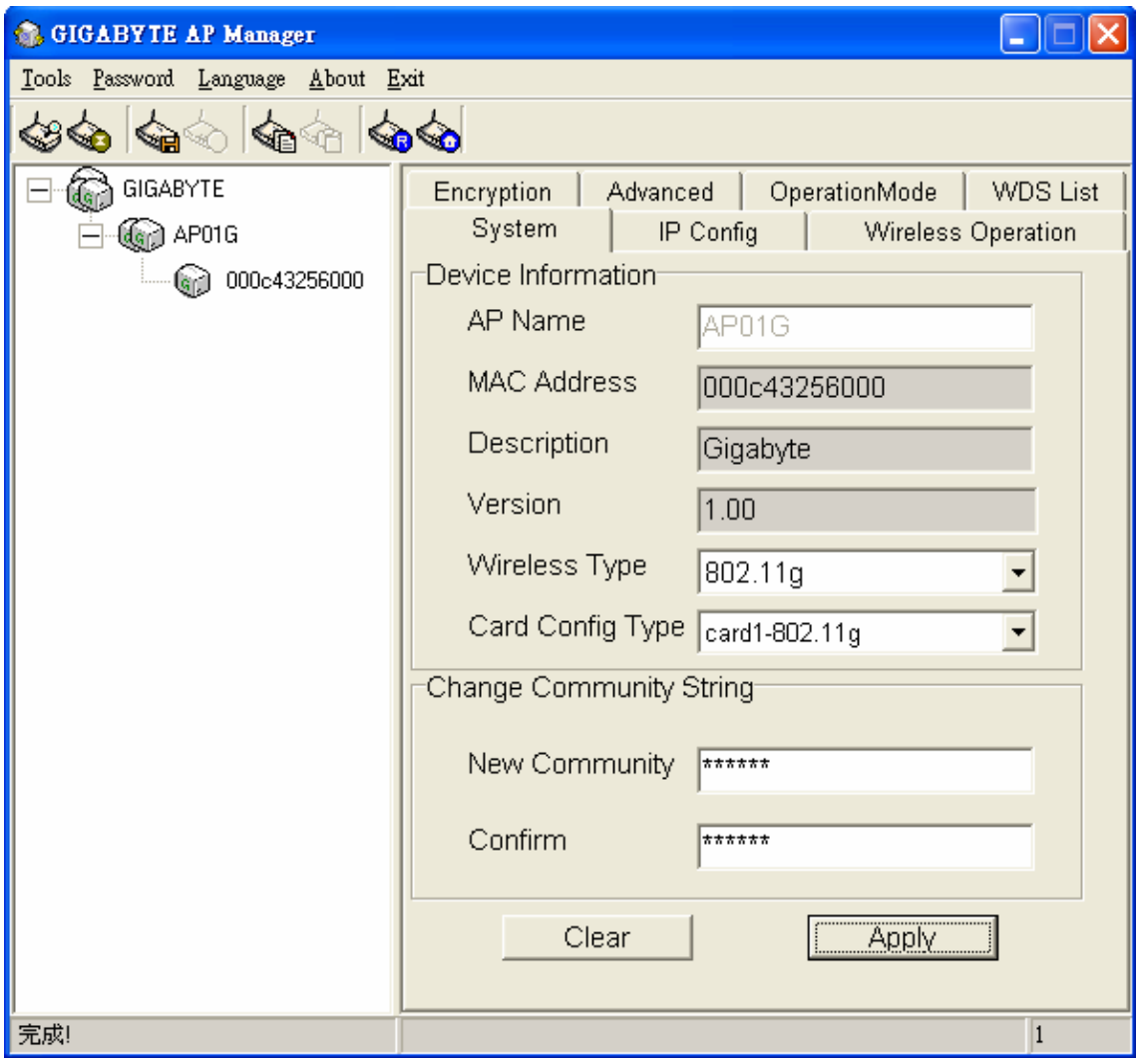
Using the Access Point Manager

You can launch Gigabyte AP Manager through **Start** \ **Programs** \ **Gigabyte AP Manager Utility** \ **Gigabyte AP Manager**.

Enter the default password "**admin**" and click "OK".



It will automatically search for Access Points on the **same subnet** when you open the Gigabyte AP Manager. You may click the icon to searching for Access Points manually.



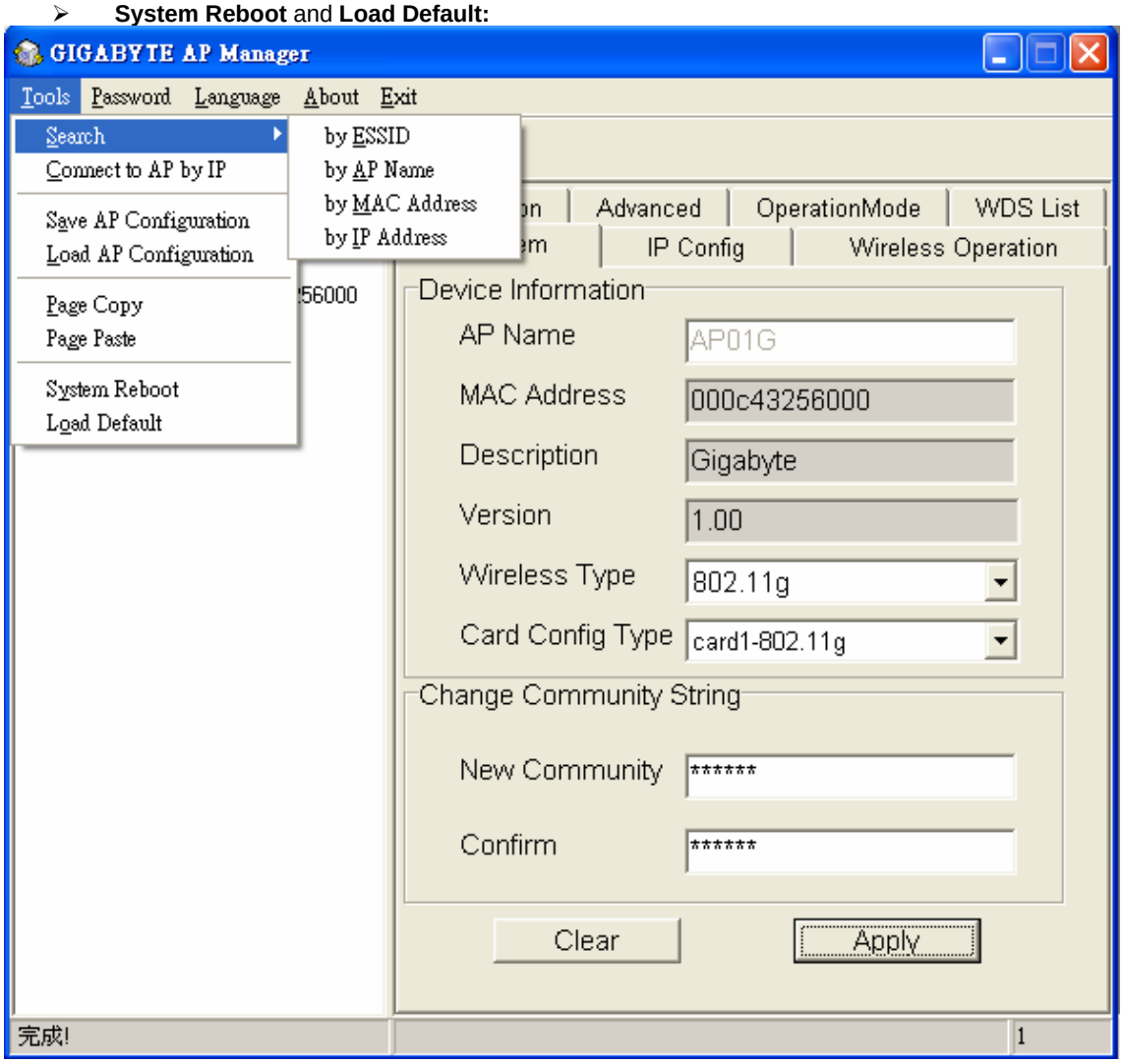
Tree structure

ESSID (GIGABYTE)
→AP Name (AP01G)
→ MAC Address (000c43256000)

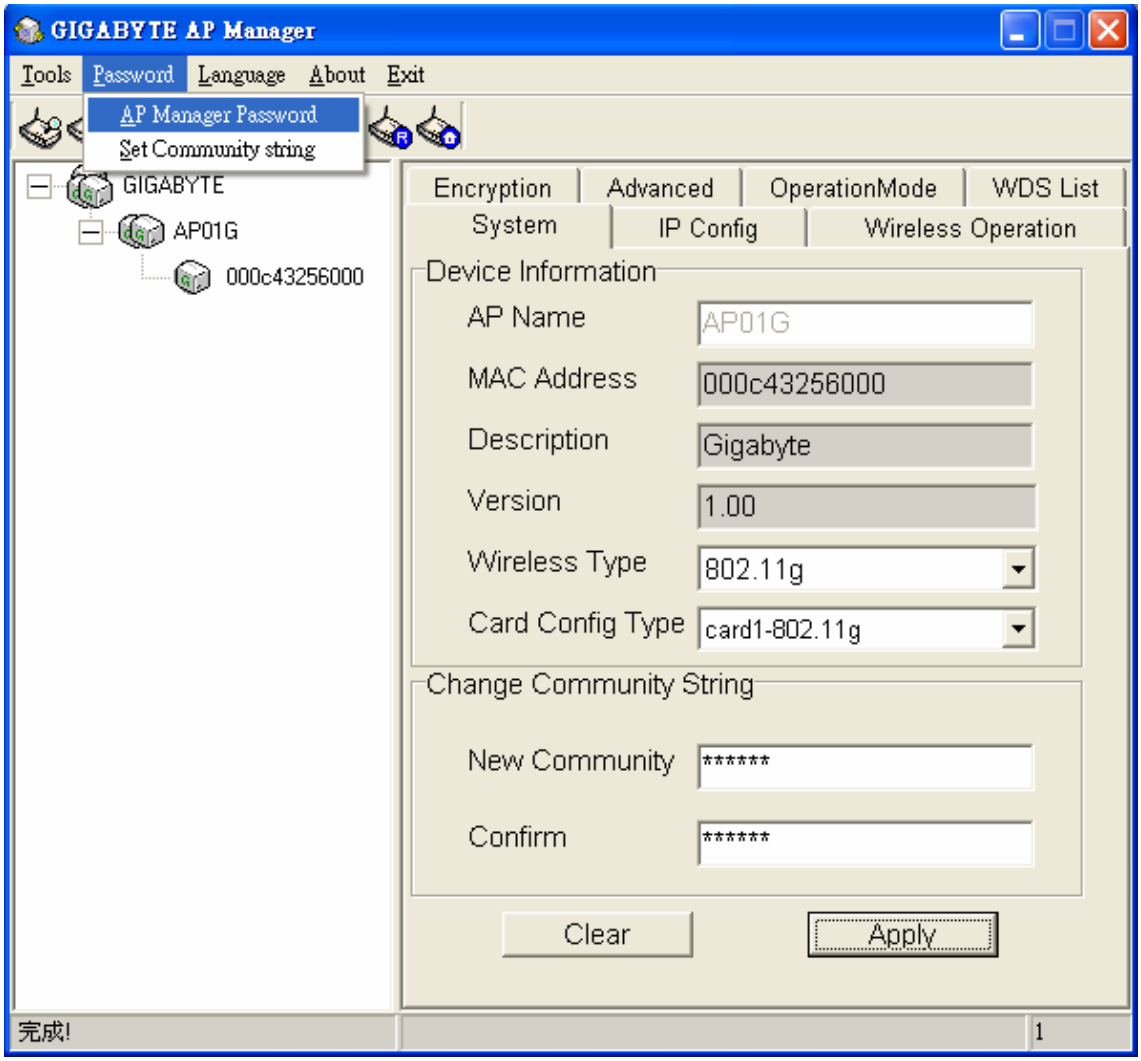
Menu bar

Tools: Including the following functions

- **Search** for AP by ESSID, AP Name, MAC Address, and IP Address
- **Connect to AP by IP:**
- **Save** and **Load** the AP configuration
- **Copy** and **Paste** the configuration
- **System Reboot** and **Load Default:**



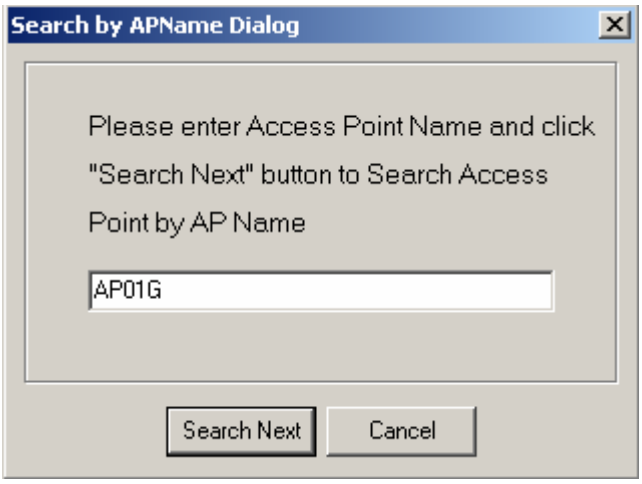
Password
Allows you to change the AP Manager password and set the SNMP community string.



About
An online help link and the version of the AP Manager.

Exit
Exit the AP Manager.

Note: *When you search for AP by AP Name (Tools->Search->By AP Name). You can press the "search next" to continue to search the same name of AP.*


Search by APName Dialog
Please enter Access Point Name and click "Search Next" button to Search Access Point by AP Name
AP01G
Search Next
Cancel

Tool bar

Find Access Point

Save AP Configuration

Page Copy

System Reboot

Connect To AP By IP

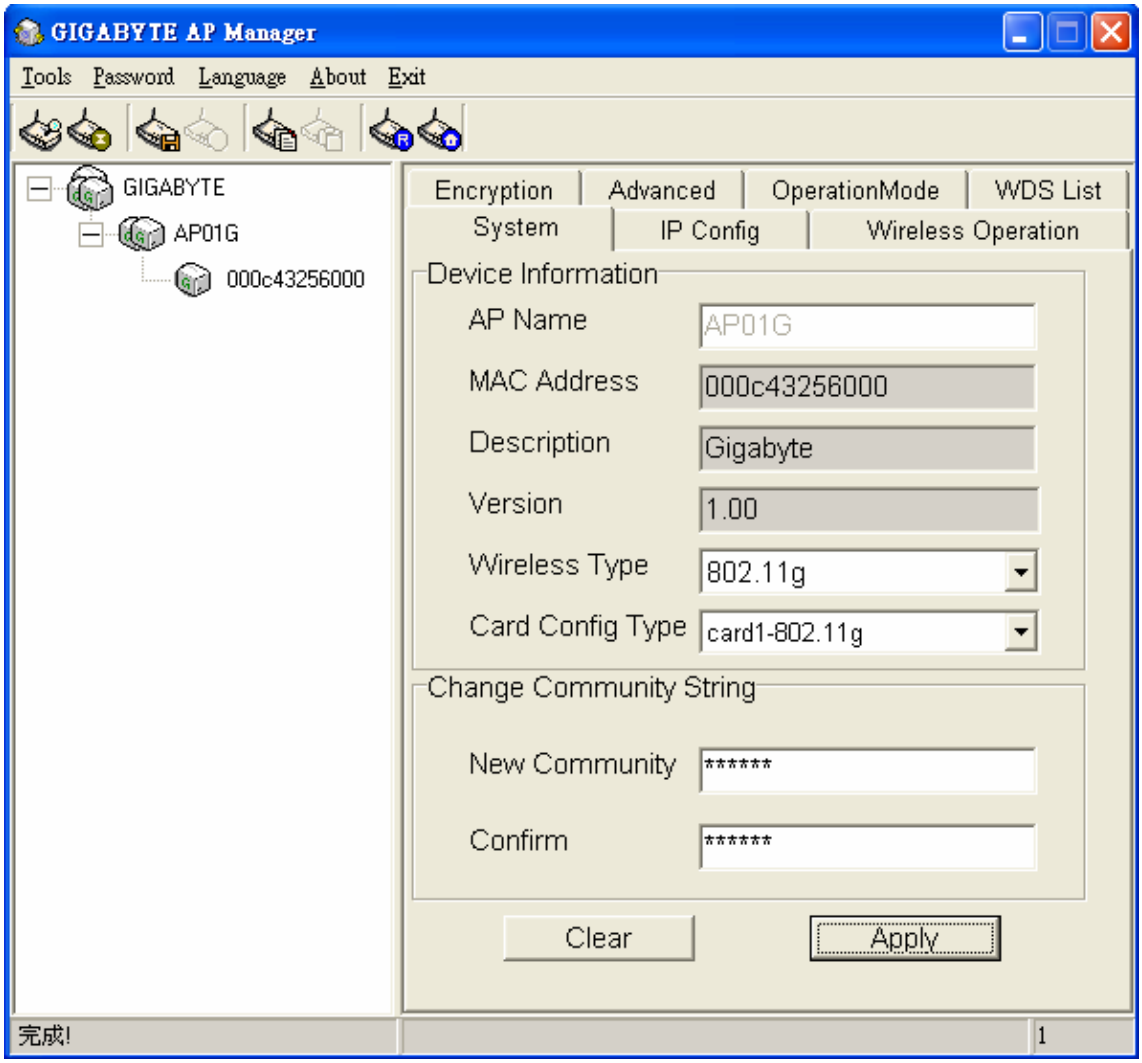
Load AP configuration

Page Paste

Load Default

- Find Access Point: Find all AP in the same subnet.
- Save AP Configuration: Save all setting of the AP to a temp file.
- Load AP Configuration: Load the setting of the temp file that you saved before to the current AP.
- Page Copy: Copy the setting of the current page.
- Page Paste: Paste the setting you have copied to the current page. (You can paste the setting of AP1 to AP2 at the same tab page.)
- System Reboot: Reboot the Access Point.
- Load Default: Set the Access Point to the manufacture default.
- Connect To AP By IP: If you want to manage the AP in the different subnet, use this function and key in the IP.

System Page



The System Page displays the Device Information and the Change Community String function.

Device Information

The Device Information includes the AP name, MAC address, Description, the version information and the device type.

Change Community String

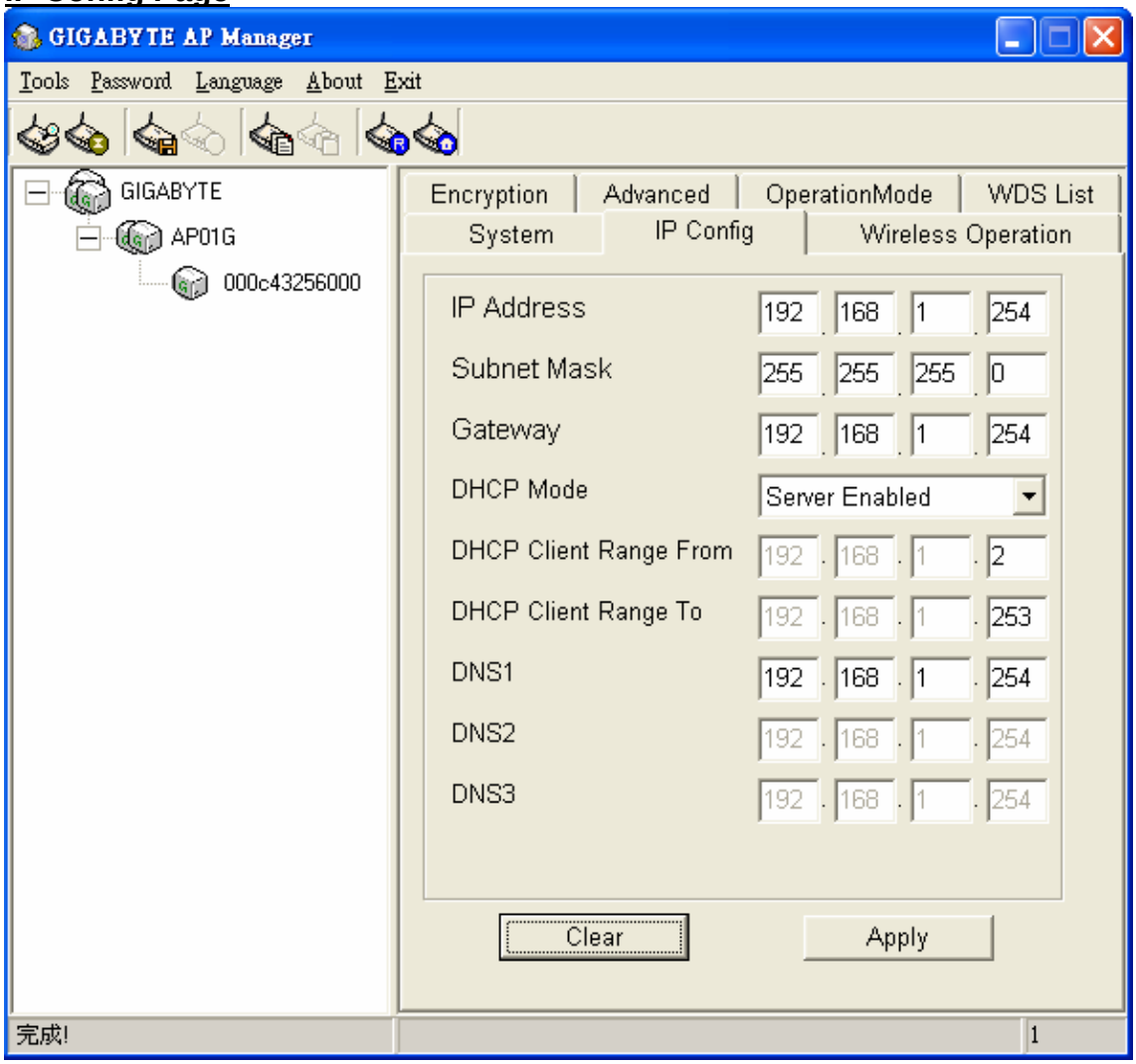
This function can let you change the community string of the AP. You can change a new community string on purpose to prohibit other AP Manager access and manage your AP. After you change the community string of the AP, you need to do the following two actions.

1. Change the Community string between Access Point and AP Manager:

   Password → *Set Community String* on the Menu Bar to change the community string of the AP manager. The AP Manager and the AP should have the same community string. Otherwise the AP Manager will not be able to find the AP with different community string
2. Please memorize the community string or write it down somewhere. In case you forget the community string, you could press the init button at the bottom of Access Point and then the AP setting (include community string) will be restored to default value.

Note: *The SNMP community string defines the relationship between an SNMP manager system (AP Manager) and the agent systems (all Access Points). This string acts like a password to control the AP Manager to access the AP. The default value of the community string is "public". You can change the community string of AP Manager by using Password->Set Community String on the Menu Bar.*

IP Config Page



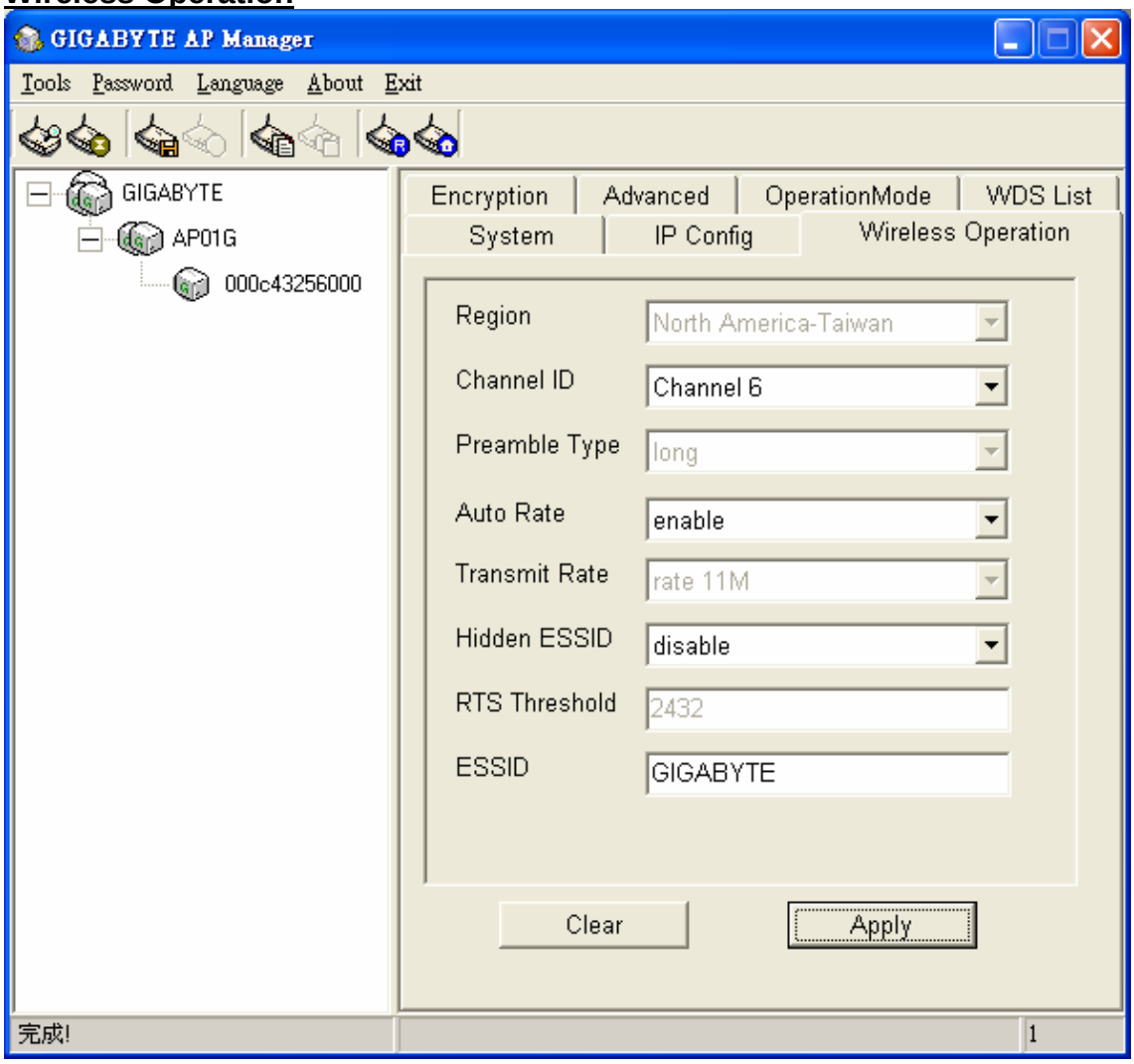
Obtain an IP address automatically

You can check this selection to get IP address from the DHCP server automatically in you network.

Use the following IP address

You can check this selection to assign IP address by yourself. The default IP address is **192.168.1.1** and the subnet mask is 255.255.255.0. Please make sure the assigned IP address is unique in your network. After you change the IP address of the AP, please also change the PC's (AP Manager) IP address to the **same subnet**. And then click the "Find Access Point" icon; AP manager will search the AP in the network.

Wireless Operation



Normally, you can have the wireless work smoothly even if you didn't change any items in this page.

Region

Because of the different region has a different open channel regulation, please check whether the default region value is your local area. If it did not appear properly region please contact your local distributor or authorized reseller immediately.

Channel ID

Please choose the channel for best performance. Normally, no change is needed. The default value is channel 6.

Preamble Type

The preamble field shall be provided so that the receiver can perform the necessary operations for synchronization.

Transmit Rates

Select the desired data rate. The range is from 1 to 54Mbps and the default rate is set to "Auto".

Auto Rate

In this item you can select either "enable" or "disable". The default value is "enable".

Enable: If the selection is "enable", the transmit rates will automatically change to the optimum rate allowed. The range of auto-change will base on the setting of "Transmit Rate".

Disable: There is no transfer rate auto-change. The transfer rate will be defined by the "Transmit Rate" column.

Hidden ESSID

This setting enables you to hide ESSID name, which is needed by clients in order to connect to the Access Point. The default value is **"Disable"**. In this setting, ***all users are able to read your AP's SSID name.***

RTS Threshold

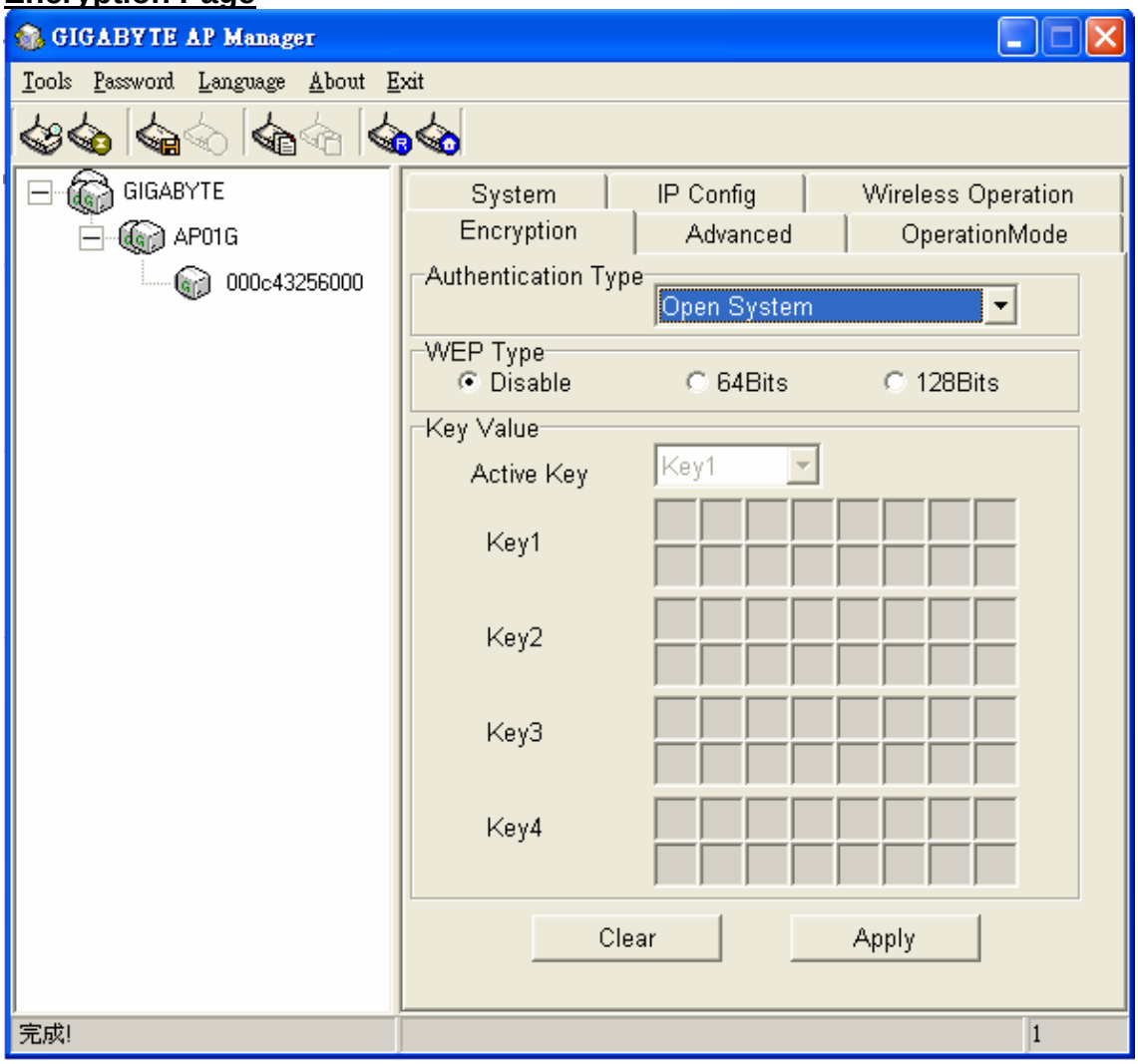
This value should remain at its default setting of 2432.

ESSID

ESSID (or SSID as it is usually referred to) is the network name of the Access Point in the wireless network. You should set the same SSID name for all your wireless-equipped devices to allow dynamic clients to easily roam among them. The SSID name can be up to 32 characters in length and is case sensitive (i.e. upper case letters **"A~Z"** and lower case **"a~z"** are unique).8

Verify the desired setting and then click the "**Apply**" button to set the value into Access Point.

Encryption Page



This page is the security configuration of the wireless connection. WEP (Wired Equivalent Privacy) is a data privacy mechanism based on a 64/128-bit shared key algorithm, as described in the IEEE 802.1x standard. When the “Disable” is selected, there is no WEP encryption. When either “64bits” or “128bits” is selected there is encrypted data transfer to prevent unauthorized users accessing the wireless network.

■ Authentication Type
The Authentication Type default is set to “Open system”.

*** Open system**

Allows any device to connect to the network, assuming the device’s SSID matches the access point’s SSID.

*** Shared Key**

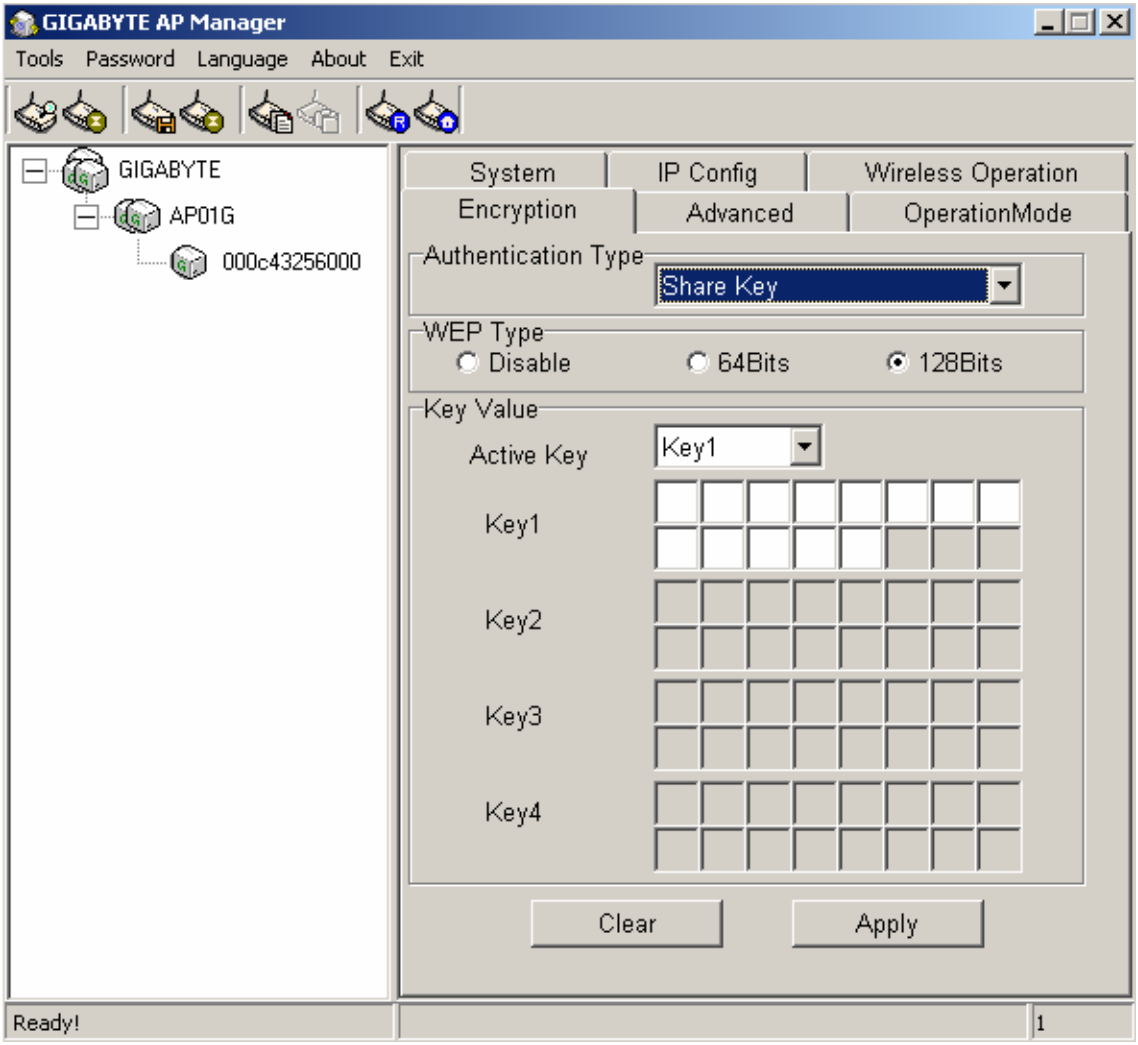
Only those computers that have the correct authentication key can join the network.

Key Length choice

Disable - No encryption will be applied.

64-bit - enter 5 hexadecimal digits.

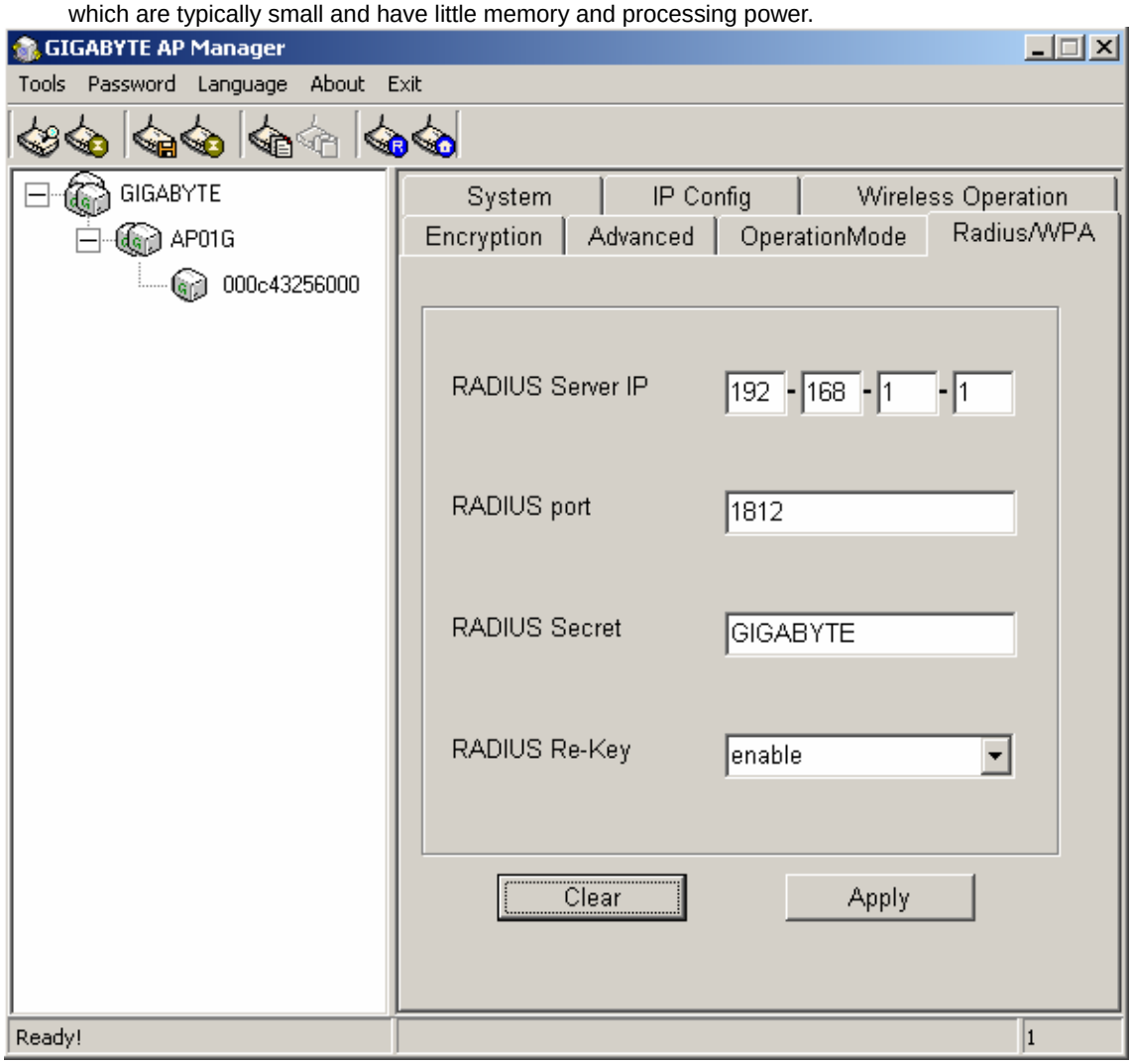
128-bit - enter 13 hexadecimal digits.



Verify the desired setting and then click the "**Apply**" button to set the value into access point.

*** 802.1x**

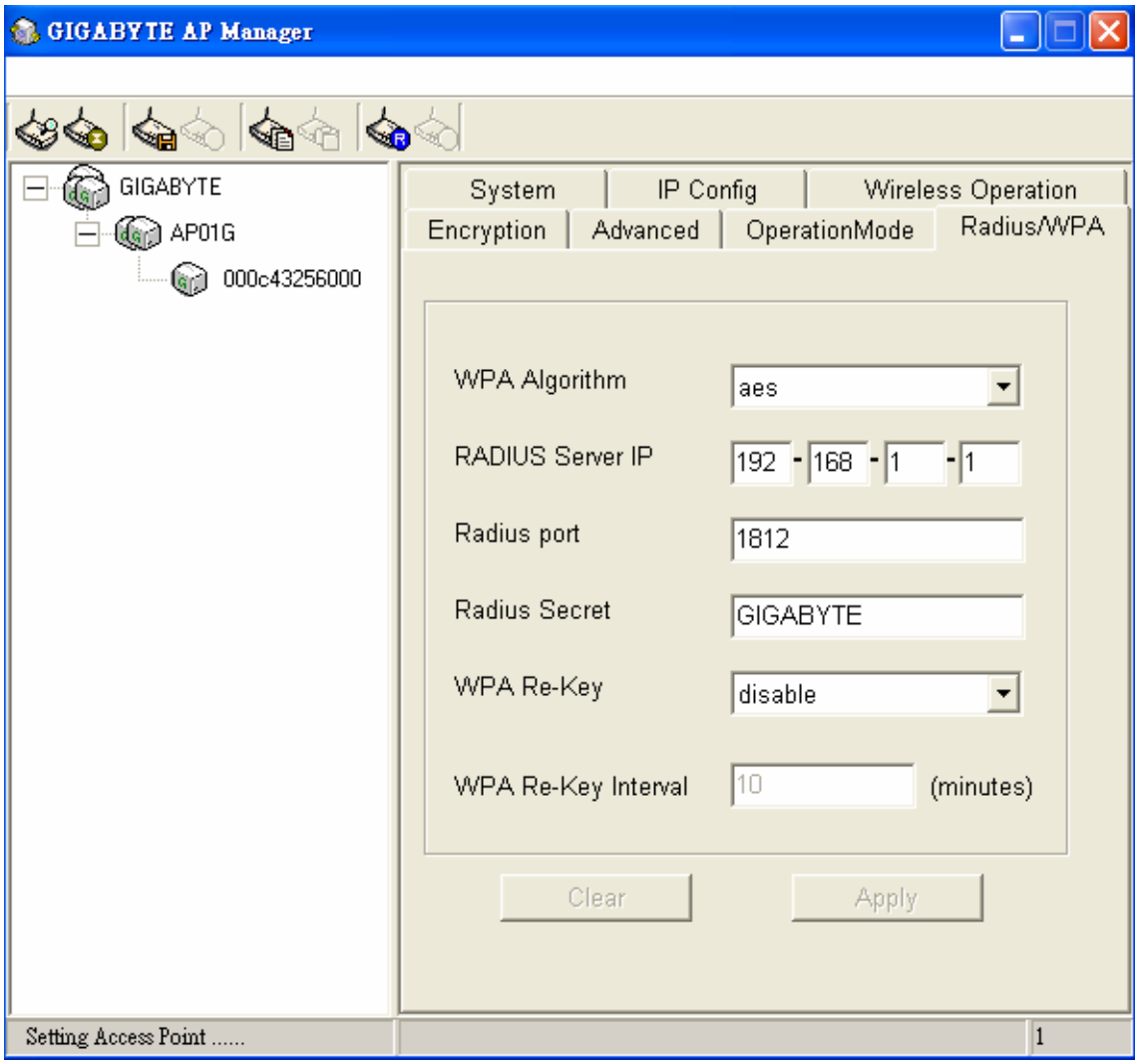
802.1x is IEEE standard for EAP encapsulation over wired or wireless Ethernet. 802.1x uses three terms that you need to know. The user or client that wants to be authenticated is called a supplicant. The actual server doing the authentication, typically a RADIUS server, is called the authentication server. And the device in between, such as a wireless access point, is called the authenticator. One of the key points of 802.1x is that the authenticator can be simple and dumb - all of the brains have to be in the supplicant and the authentication server. This makes 802.1x ideal for wireless access points, which are typically small and have little memory and processing power.



RADIUD Server IP – Assign an IP address for the RADIUS Server.
RADIUS Port – Enter a value within the range 1~65536 for port.
RADIUS Secret – Enter a password up to 32 ASCII characters (uppercase “A~Z”, lowercase “a~z”, or numeric “0~9”) in length.
RADIUS Re-key – Lets you enable or disable the RADIUS Re-Key function.

*** WPA (Wi-Fi Protected Access)**

If you have used Wi-Fi for a while, you may be familiar with 802.1x Authentication Protocol, which allows users to authenticate the wireless network via RADIUS server. The 802.1x Authentication Protocol is an option in standard Wi-Fi but a must for WPA.

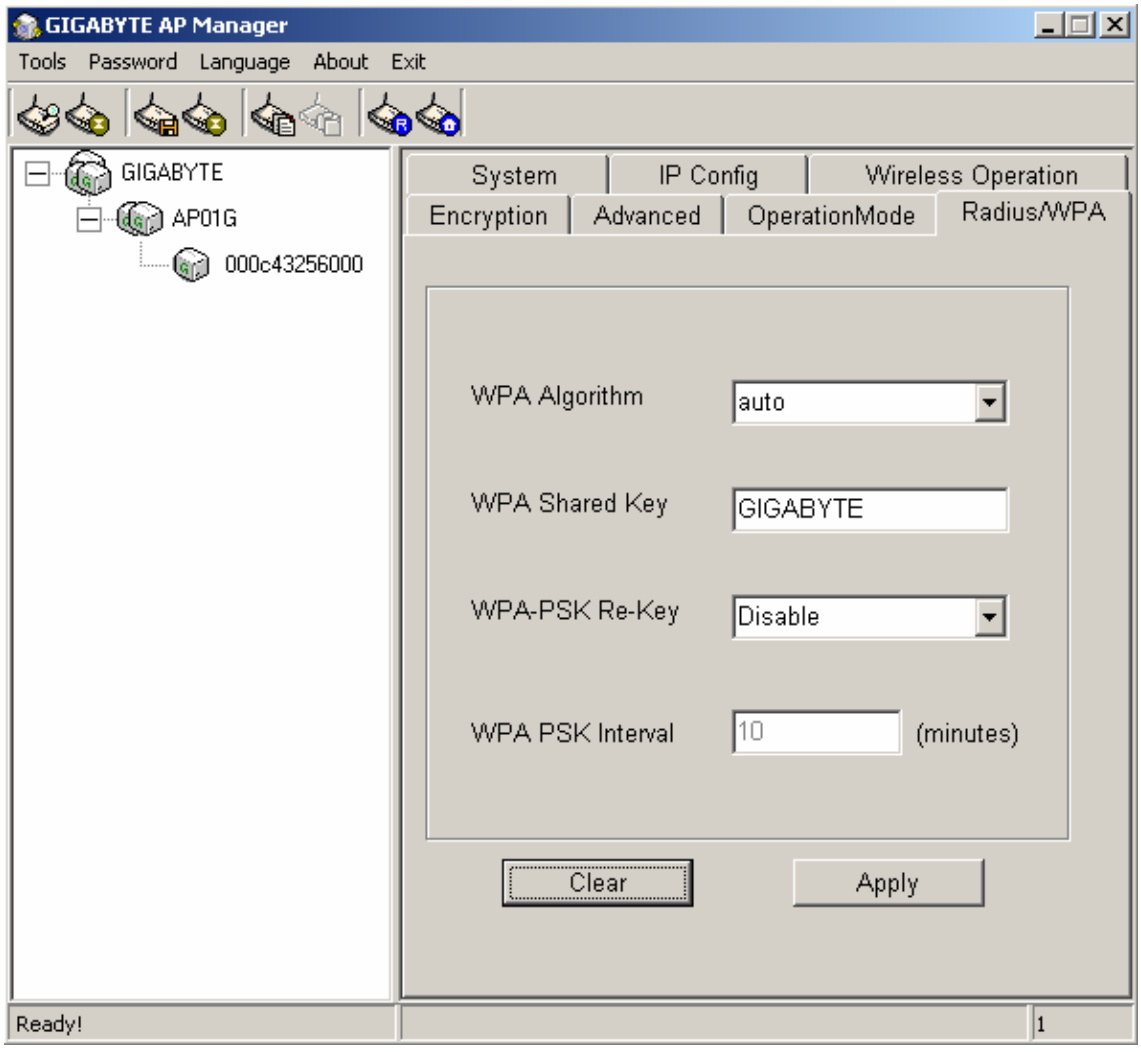


RADIUD Server IP – Assign an IP address for the RADIUS Server.
RADIUS Port – Enter a value within the range 1~65536 for port.
RADIUS Secret – Enter a password up to 32 ASCII characters (uppercase “A~Z”, lowercase “a~z”, or numeric “0~9”) in length.
RADIUS Re-key – Lets you enable or disable the RADIUS Re-Key function.
Cipher Algorithms – Two options you can choose: TKIP and AES settings.
Group Re-key - Lets you enable or disable the RADIUS Re-Key function.

*** WPA Pre-Shared Key**

Traditional WEP had an inconvenient method to change encrypted keys. Even when you changed the encrypted keys; you still can not select all APs and wireless LAN adapter while you are changing encrypted keys.

The manual re-keying which is necessary with WEP is a tedious manual process and is completely impractical for large organizations. After all, the instant you re-key an access point, none of the clients will be able to access it until they too are re-keyed. But with WPA, the re-keying of global encryption keys is all that is necessary. In the case of unicast traffic, the encryption key is changed after every frame using Temporary Key Integrity Protocol (TKIP). This protocol allows key changes to occur on a frame-by-frame basis and to be automatically synchronized between the access point and the wireless client. Global re-keying works by advertising the new keys to wireless clients.

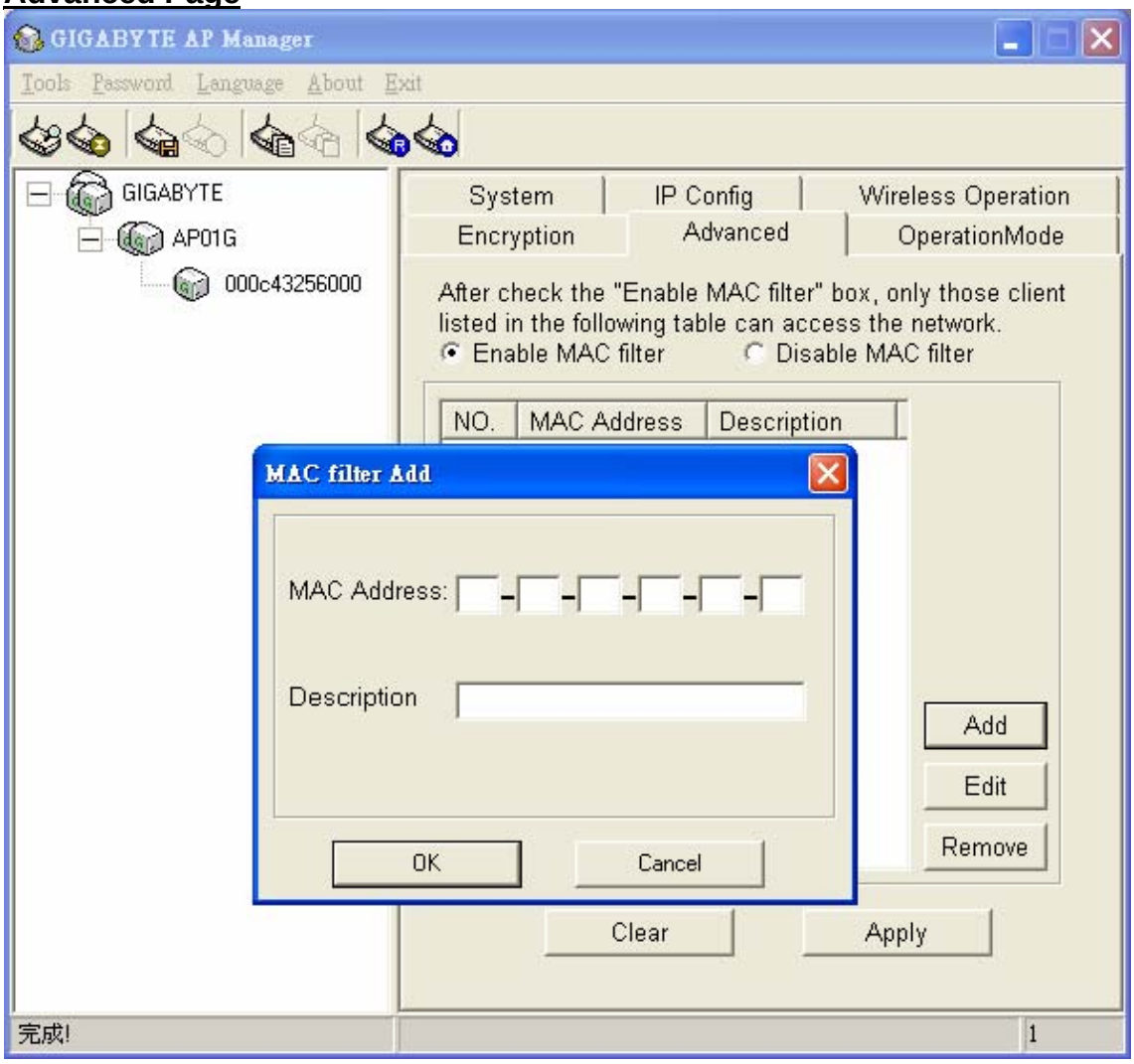


Cipher Algorithms – Two options you can choose: TKIP and AES settings.

Group Re-key - Two options: Enabled or Disabled.

Pre-Shared key - Enter a password up to 63 ASCII characters (uppercase “A~Z”, lowercase “a~z”, or numeric “0~9”) in length.

Advanced Page



To enhance the security of the wireless network, this AP provide the MAC address filtering mechanism to prevent the unauthorized user access. Check “Enable MAC filter” and key in MAC address table, then only those MAC address in the table are allowed to connect to this AP.

■ Enable MAC Filter
Choose the “Enable MAC Filter” and click the “**Add**” button to add more MAC addresses or click “**Remove**” button to delete the MAC addresses from the Authorized MAC Address table. Besides, you can click “**Edit**” button to edit the MAC address.

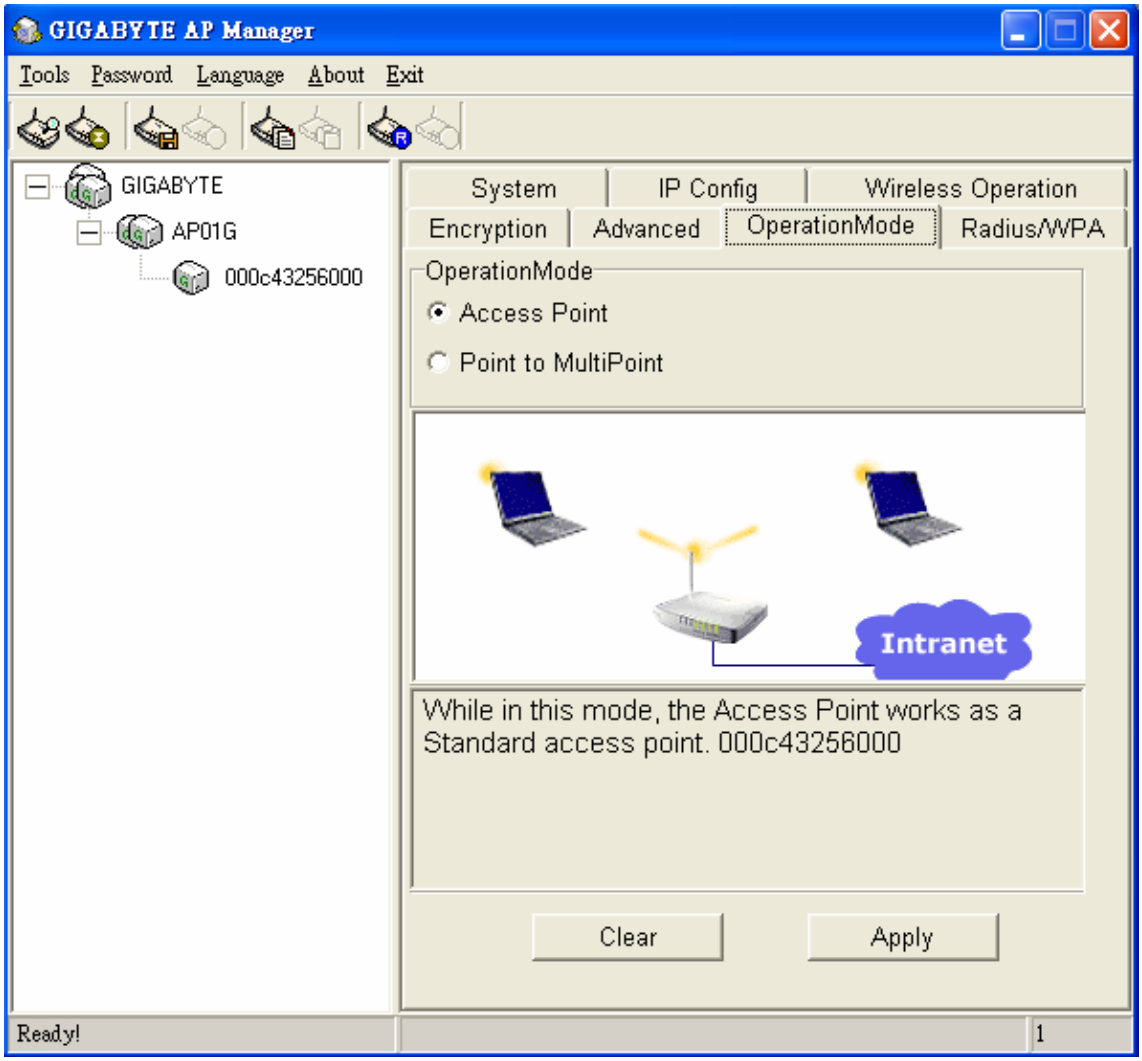
■ Disable MAC Filter
The default is “Disable MAC filter".

Verify the desired setting and then click the “**Apply**” button to set the value into access point.

Operation Mode Page

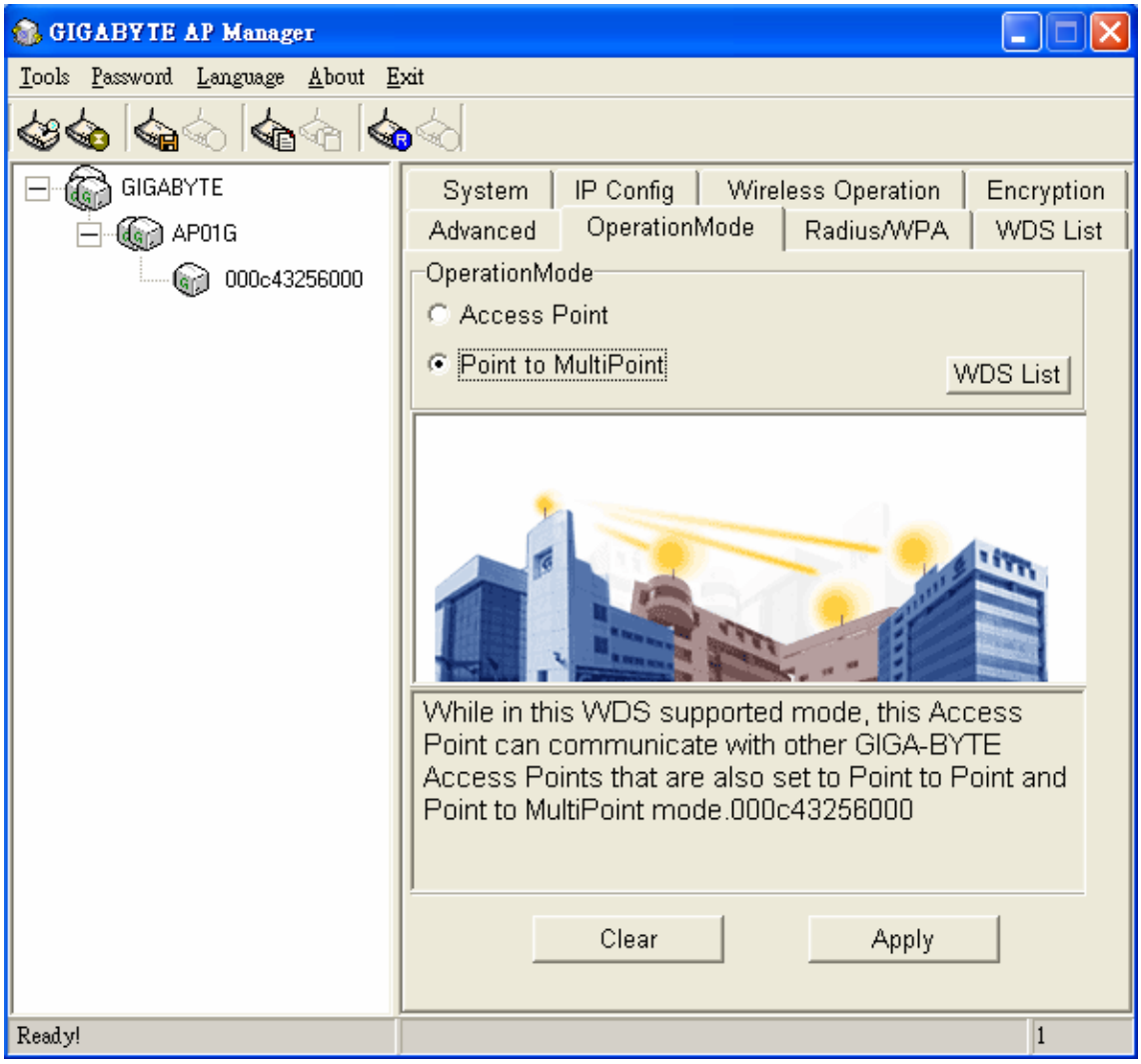
The Access Point supports three operation modes: “Access Point”, “Point to Point”, “Point to MultiPoint”. The default operation mode is “Access Point”.

Access Point Mode



In this operation mode, the Access Point works as a Standard 802.11g based access point.

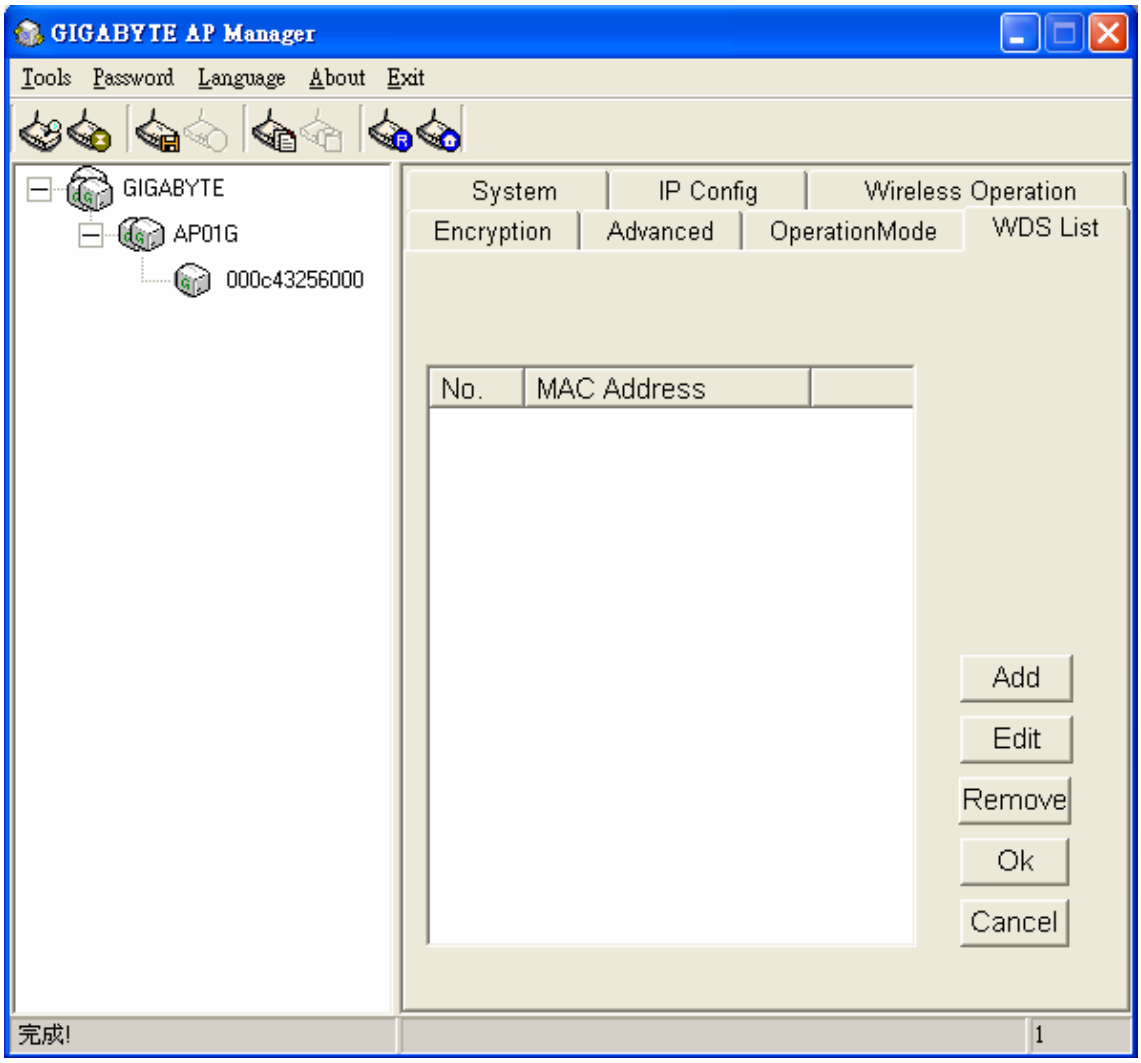
Point to MultiPoint Mode



In this WDS supported mode, the Access Point can communication with other GIGABYTE Access point which is also set to Point to Point and MultiPoint mode.

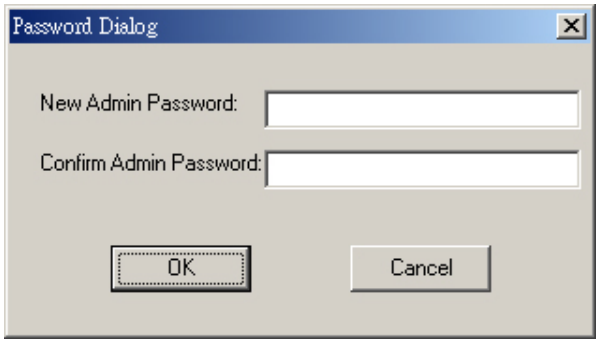
WDS List

After selecting the Point to MultiPoint Mode, you have to add the MAC address of Access Point on the WDS List



Change AP Manager Password

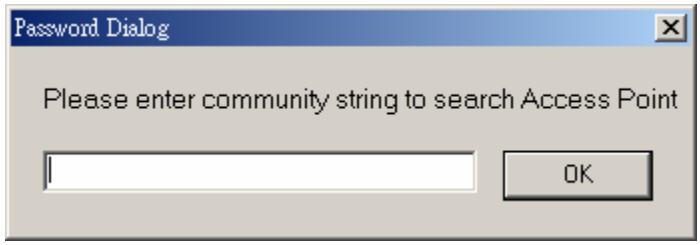
User can change the administration password of the AP manger to prevent other user access to the AP Manager. On the Menu Bar (Password->AP Manager Password) can invoke the password change dialog. Please enter a new admin password and confirm admin password then press “OK”. You have to enter this new password to log in when you want to use the AP Manager next time.



Set Community String

The community string defines the relationship between AP manager and the AP. This string acts like a password to control the AP Manager to access the AP. For detail description, please refer to “System Page” section.

Please enter a community string and then press “OK”.



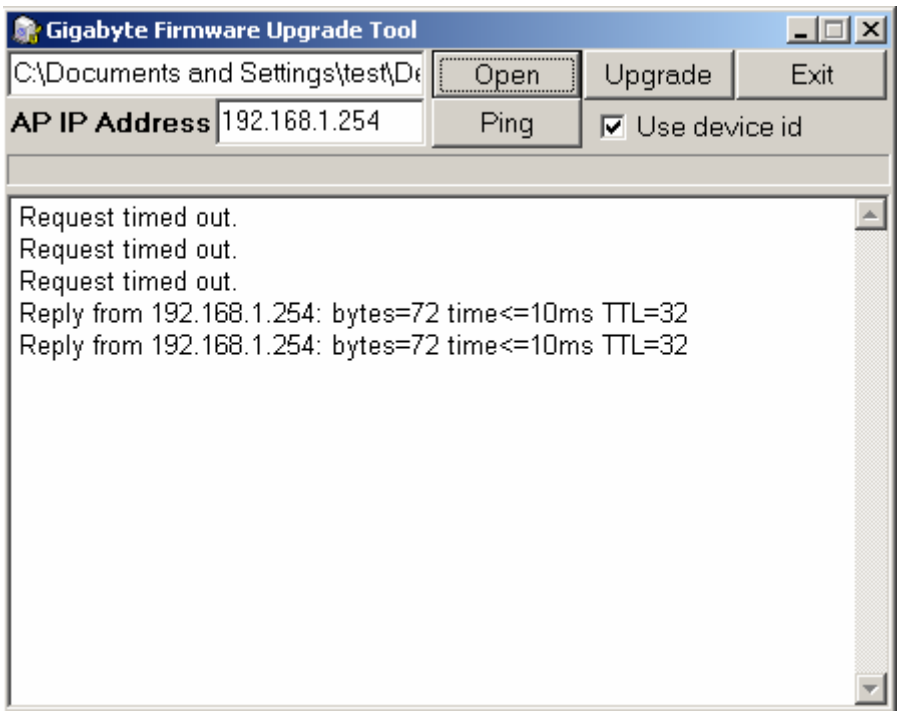
Upgrade Firmware

You can download the upgraded firmware version from Gigabyte website.

■ Run TFTP Program

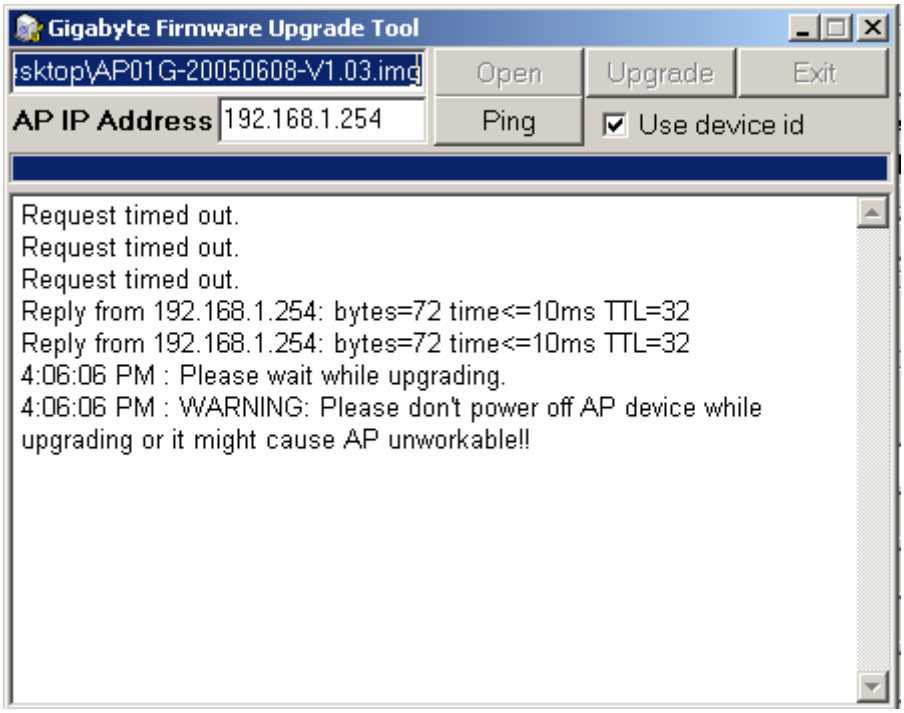
Step1. You can find the “Upgrade Tool” through **Start** \ **Programs** \ **Gigabyte AP Manager Utility** \ **Gigabyte AP Upgrade**.

Step2. The Gigabyte Firmware Upgrade Tool screen will appear. Please enter the “AP IP address” which you want to upgrade the firmware. You can press “**Ping**” button to verify whether the AP is online.

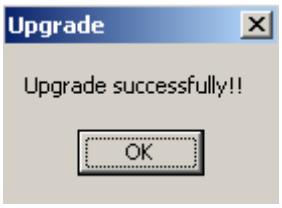


Step3. Press "**Open**" button to choose the firmware then press "**Upgrade**" button to start the firmware upgrade process.

Note: *During the firmware upgrade, please* ***DO NOT*** *turn off the PC or AP and* ***DO NOT*** *unplug the Ethernet cable.*



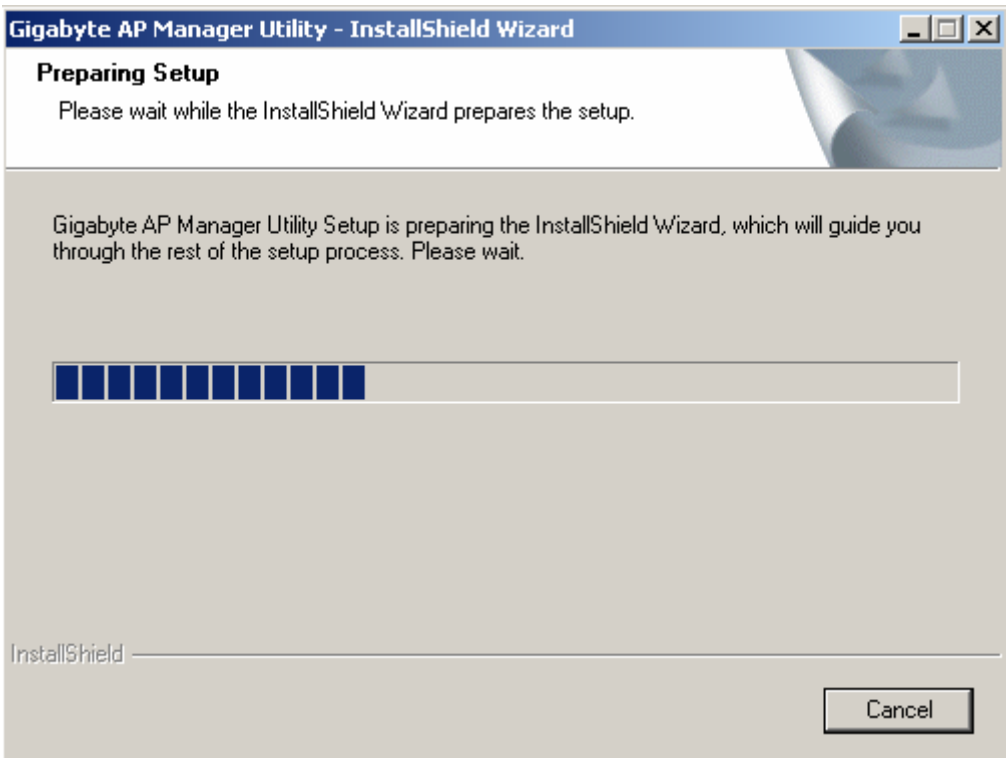
Step4. After the AP device rebooting successful, the AP firmware upgrade is completed.



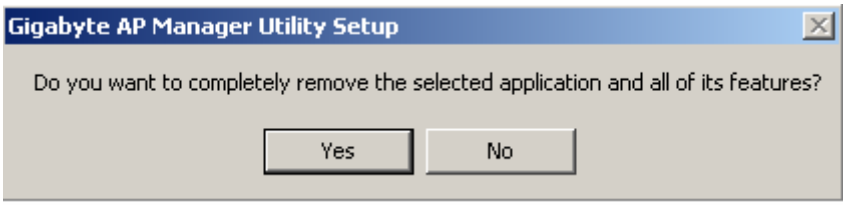
Uninstall AP Manager Utility

You can find the Uninstall program through **Start** \ **Programs** \ **Gigabyte AP Manager Utility** \.

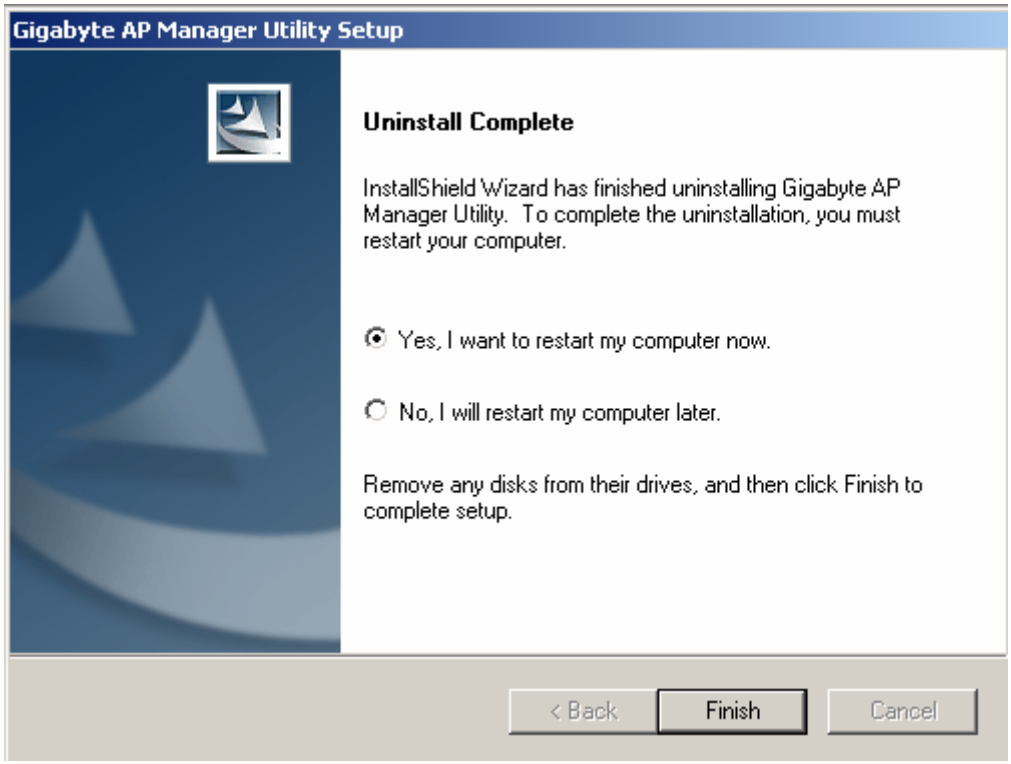
Step1. The InstallShield Wizard will appear then please wait.


Gigabyte AP Manager Utility - InstallShield Wizard
Preparing Setup
Please wait while the InstallShield Wizard prepares the setup.
Gigabyte AP Manager Utility Setup is preparing the InstallShield Wizard, which will guide you through the rest of the setup process. Please wait.
InstallShield
Cancel

Step2. Click "**Yes**".

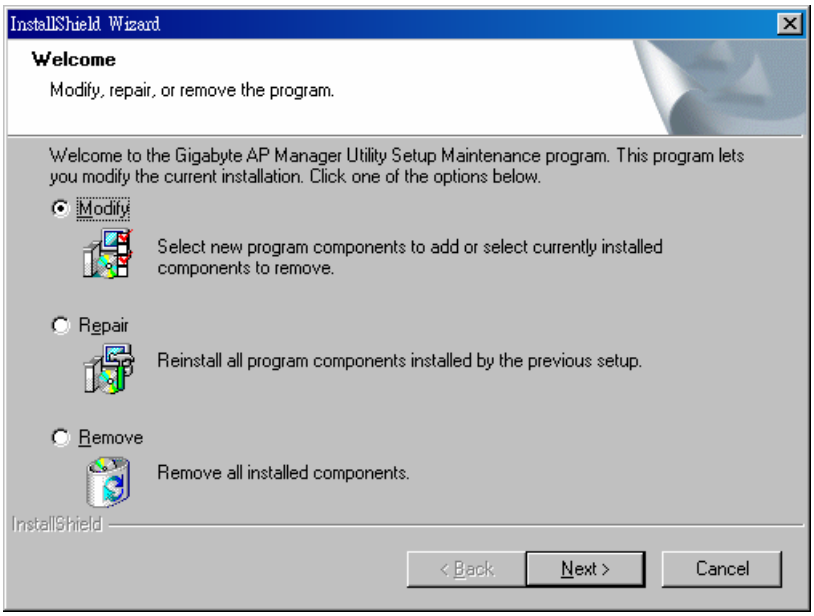

Gigabyte AP Manager Utility Setup
Do you want to completely remove the selected application and all of its features?
Yes
No

Step3. Click “Finish” to restart the computer and then the Gigabyte AP Manager Utility has been uninstalled successfully.


Gigabyte AP Manager Utility Setup
Uninstall Complete
InstallShield Wizard has finished uninstalling Gigabyte AP Manager Utility. To complete the uninstallation, you must restart your computer.
Yes, I want to restart my computer now.
No, I will restart my computer later.
Remove any disks from their drives, and then click Finish to complete setup.
< Back
Finish
Cancel

If you just want to modify some program components or reinstall all program components, you can run the installation program directly. And then the InstallShield Wizard will appear.

Please choose one of the options what you want then click “**Next**” continues to modify, repair or remove the Gigabyte AP Manager Utility.


InstallShield Wizard
Welcome
Modify, repair, or remove the program.
Welcome to the Gigabyte AP Manager Utility Setup Maintenance program. This program lets you modify the current installation. Click one of the options below.
Modify
Select new program components to add or select currently installed components to remove.
Repair
Reinstall all program components installed by the previous setup.
Remove
Remove all installed components.
InstallShield
< Back
Next >
Cancel

Chapter 5 Troubleshooting

This chapter gives information about troubleshooting your AirCruiser G Access Point. Read the descriptions below for assistance is diagnosing and solving the problem.

Q: What to do if you forget your password or forget the IP address of the Access Point?

A: Please press and hold for 5 seconds the **"init"** button at the bottom of the Access Point. The Access Point will be reset to the factory default values, and the password will be restored to factory default.

Q: I am unable to connect to the Internet.

A:
1. Confirm that the power cord is connected properly and the Access Point's power LED is correctly lit.
2. Check whether all of the settings described in this manual are correctly set.
3. Verify that your ADSL/Cable Modem is operating normally, and/or you have ISP service available.
4. Check that your network cable is connected correctly, and the LED status is normal.

Q: I am unable to access the Access Point's Web Configuration Interface.

A:
1. Please check the Ethernet connection (RJ-45 LAN cable) between the PC and the Access Point is properly connected.
2. Make sure your computer's IP address is on the same subnet as the Access Point. (Check this by typing `ipconfig /all` from a DOS command prompt)
3. Make sure you are carefully typing the correct IP address of the router in the address bar of your web browser. The IP address of your router is the "Gateway" address you see when you run the `ipconfig /all` command.
4. Try initializing your router to factory settings.

Q: What is the IEEE 802.11b standard?

A: It is also referred to as 802.11 High Rate or Wi-Fi. It is an expansion to 802.11 that applies to wireless LAN and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. The 802.11b uses only Direct Sequence Spread Spectrum (DSSS). The 802.11b was a 1999 ratification to the origianl 802.11 standard, allowing wireless functionality comparable to Ethernet.

Q: What is WEP?

A: Wired Equivalent Privacy (WEP). A security mechanism defined within the 802.11 standard and designed to make the link integrity of the wireless medium equal to wired cable.

Q: What is the IEEE 802.11g standard?

A: IEEE 802.11g standard specifies data rates of up to 54 Mbps in the 2.45-GHz band. It uses Orthogonal Frequency Division Multiplexing (OFDM), which is the mandatory provisions have been made within the standard to make it inherently compatible with the well-established 802.11b standard at 11 Mbps, which uses Complementary Code Keying (CCK) modulation. Both .11g and .11b can operate at ranges of up to 300 feet.

Appendix A: Glossary

10BaseT
The most common cabling method for Ethernet. 10BaseT conforms to IEEE standard 802.3. It was developed to enable data communications over unshielded twisted pair (telephone) wiring at speeds of up to 10 megabits per second up to distances of approximately 330 feet on a network segment.

802.11
A group of wireless networking standards, also known as Wi-Fi, set by the Institute of Electrical and Electronics Engineers (IEEE).

802.1X
A standard for port-based authentication, first used in wired networks, that was adapted for use in enterprise WLANs to address security flaws in WEP, the original security specification for 802.11 networks. 802.1X provides a framework for authenticating users and controlling their access to a protected network and dynamic encryption keys to protect data privacy.

Access Point
An Access Point is a wired controller that sends data to the wireless NIC's installed in your network computers, and received data back from them. An Access Point is often connected to the network computer that has Internet access, or is directly connected to an ADSL or cable modem.

Ad-Hoc mode
An old term used to describe a device-to-device network. (See device-to-device network, peer-to-peer network).

ADSL
Asymmetric digital subscriber line (ADSL) is a new modem technology that converts existing twisted-pair telephone lines into access paths for high-speed communication of various sorts.

AES
Advanced Encryption Standard. The preferred standard for the encryption of commercial and government data using a symmetric block data encryption technique. It is used in the implementation of WPA2.

Auto-MDI/MDIX
On a network hub or switch, an auto-MDI/MDIX port automatically senses if it needs to act as a MDI or MDIX port. The auto- MDI/MDIX capability eliminates the need for crossover cables.

Auto-negotiate
To automatically determine the correct setting. The term is often used with communications and networking.

Bridge
A wireless device that connects multiple networks together.

BSSID
Basic Service Set Identifier. A unique address that identifies the access point/router that creates the wireless network.

Channel
One portion of the available radio spectrum that all devices on a wireless network use to communicate. Changing the channel on the access point/router can help reduce interference.

Client
Any computer connected to a network that requests files and services (files, print capability) from the server or other devices on the network. The term also refers to end users.

Client devices
Wi-Fi client devices include PC Cards that slide into laptop computers, mini-PCI modules embedded in laptop computers and mobile computing devices, as well as USB radios and PCI/ISA bus Wi-Fi radios. Client devices usually communicate with hub devices like access points and gateways.

DHCP
The Dynamic Host Configuration Protocol (DHCP) is an Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses, to deliver TCP/IP stack configuration parameters such as the subnet mask and default router, and to provide other configuration information such as the addresses for printer, time and news servers.

DSSS
Also known as “Direct Sequence Spread Spectrum,” this is a variety of radio transmission methods that continuously change frequencies or signal patterns. Direct Sequence Spread Spectrum (DSSS), which is used in CDMA technology,. multiplied the data bits by a very fast, pseudo-random bet pattern (PN sequence) that “spreads” the data into a large coded stream that takes the full bandwidth of the channel.

DNS
The Domain Name System (DNS) is a distributed Internet directory service.DNS is used mostly to translate between domain names and IP addresses, and to control Internet email delivery. Most Internet services rely on DNS to work, and if DNS fails, web sites cannot be located and email delivery stalls.

Dynamic IP Address
An IP address is automatically assigned to a user’s AP in a TCP/IP network typically by a DHCP server.

EAP
Extensible Authentication Protocol. A protocol that provides an authentication framework for both wireless and wired Ethernet enterprise networks. It is typically used with a RADIUS server to authenticate users on large networks. EAP protocol types are used in the 802.1X-based authentication in WPA-Enterprise and WPA2-Enterprise.

Encryption
A mechanism for providing data confidentiality.

Ethernet
The most popular international standard technology for wired Local Area Networks (LANs). It provides from 10 Mbps transmission speeds on basic 10BastT Ethernet networks to 100 Mbps transmission speeds on Fast Ethernet networks, 1000 Mbps on Gigabit Ethernet, and 10,000 Mbps on 10 Gigabit Ethernet.

Firewall
A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets.All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Firmware
Software routines that are embedded as read-only memory (ROM) in a computer chip or hardware device to prevent modification of the routines. Unlike random access memory (RAM), read-only memory stays intact in the absence of electrical power. Startup routines and low-level input/output instructions are stored in firmware.

Gateway
A device, usually a Router, that connects hosts on a local network to other networks.

Infrastructure mode

An old term used to describe a wireless network consisting of devices connected to a network using a centralized wireless access point. One of two types of wireless network modes; the other is a device-to-device network (also known as peer-to-peer or ad hoc mode).

IP Address
Every PC on the Internet has a fixed identifying number, called a IP Address. A typical IP address looks like this: 216.27.61.137

LAN
A system of connecting PCs and other devices within the same physical proximity for sharing resources such as an Internet connections, printers, files and drives. When Wi-Fi is used to connect the devices, the system is known as a wireless LAN or WLAN.

MAC Address
On a local area network (LAN) or other network, the MAC (Media Access Control) address is your computer's fixed hardware number.Usually written as: 01:23:45:67:89:ab

Ping (Packet Internet Groper)
A utility to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply. PING is used primarily to troubleshoot Internet connections.

RADIUS
Remote Access Dial-Up User Service. A standard technology used by many major corporations to protect access to wireless networks. RADIUS is a user name and password scheme that enables only approved users to access the network; it does not affect or encrypt data. The first time a user wants access to the network, secure files or net locations, he or she must input his or her name and password and submit it over the network to the RADIUS server. The server then verifies that the individual has an account and, if so, ensures that the person uses the correct password before she or he can get on the network. RADIUS can be set up to provide different access levels or classes of access. For example, one level can provide blanket access to the Internet; another can provide access to the Internet as well as to e-mail communications; yet another account class can provide access to the Net, email and the secure business file server. Like other sophisticated security technologies, RADIUS comes in a variety of types and levels.

RJ-45
Standard connectors used in Ethernet networks. They appear similar to standard RJ-11 telephone connectors. However, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

Roaming
The ability to move seamlessly from one area of Wi-Fi or cellular phone coverage to another with no loss in connectivity. Roaming also refers to the ability of road warriors to wirelessly connect to the Internet from different hotspots without confronting the array of schemes used by different providers to authorize use and track billing. Roaming agreements among providers allow mobile professionals to a single authentication and authorization scheme to have all charges resolved to a single bill.

Router
A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP network. Routers are located at gateways, the places where two or more networks connect.

Server
A computer that provides resources or services to other computers and devices on a network. Types of servers can include print servers, Internet servers, mail servers, and DHCP servers. A server can also be combined with a hub or router.

Site survey

A comprehensive facility study performed by network managers to insure that planned service levels will be met when a new wireless LAN, or additional WLAN segments to an existing network, are deployed. Site survey's are usually performed by a radio frequency engineer and used by systems integrators to identify the optimum placements of access points to insure that planned levels of service are met. Site surveys are sometimes conducted following the deployment to insure that the WLAN is achieving the necessary level of coverage. Site surveys can also be used to detect rogue access points.

SSID
The SSID is the name represents the routers and Access Point in wireless network.

Subnet Mask
A mask used to determine which subnet a IP address belongs to. An IP address has two components, the network address and the host address. Subnetting enables the network administrator to further divide the host part of the address into two or more subnets.

Switch
A type of hub that controls device usage to prevent data collisions and insures optimal network performance. A switch acts as a network traffic cop: Rather than transmitting all the packets it receives to all ports, as a hub does, a switch transmits packets to only the receiving port.

TCP/IP
TCP/IP (Transmission Control Protocol/Internet Protocol), the suite of communications protocols used to connect hosts on the Internet.

TKIP
Temporal Key Integrity Protocol. The wireless security encryption mechanism in Wi-Fi Protected Access. TKIP uses a key hierarchy and key management methodology that removes the predictability that intruders relied upon to exploit the WEP key. It increases the size of the key from 40 to 128 bits and replaces WEP's single static key with keys that are dynamically generated and distributed by an authentication server, providing some 500 trillion possible keys that can be used on a given data packet. It also includes a Message Integrity Check (MIC), designed to prevent an attacker from capturing data packets, altering them and resending them. By greatly expanding the size of keys, the number of keys in use, and by creating an integrity checking mechanism, TKIP magnifies the complexity and difficulty involved in decoding data on a Wi-Fi network. TKIP greatly increases the strength and complexity of wireless encryption, making it far more difficult—if not impossible—for a would-be intruder to break into a Wi-Fi network.

USB
A high-speed bidirectional serial connection between a PC used to transfer data between the computer and peripherals such as digital cameras and memory cards. The USB 2.0 specification, announced in 2000, provides a data rate of up to 480 Mbps, 40 times faster than the original specification which provided only 12 Mbps.

WAN
Wide Area Network, a communication network that covers a relatively broad geographic area, consisting of two or more LANs. Broadband communication over the WAN is often through public networks such as the ADSL or Cable systems, or through leased lines or satellites. To simplify it, please image network as a WAN.

WEP
WEP (Wired Equivalent Privacy) is a data privacy mechanism based on a 64/128-bit shared key algorithm, as described in the IEEE 802.11 standard.

Appendix B: Specifications

Physical Interface

The Wireless Access Point includes one Ethernet LAN port, one Initialize button and one antenna.

Item	Contents	Description
1.	Ethernet port	10/100Mbps Ethernet RJ-45 with auto-sensing and auto MDI/MDIX
2.	Init button	Device reset (Init to factory default)
3.	Wireless antenna	External, 2dBi
4.	Power adaptor	7.5V, 800mA

Specifications

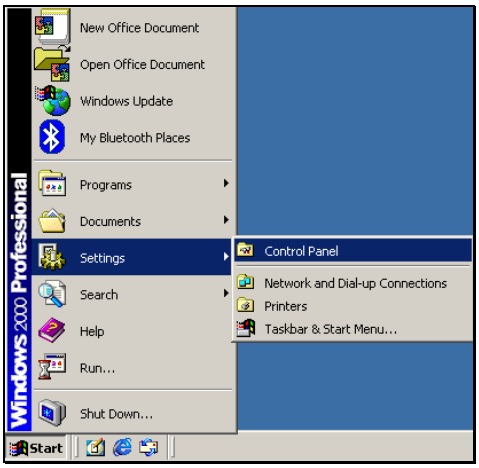
System	
CPU, Flash and SDRAM Size	RDC R2600, 1MB Flash, 8MB SDRAM
Standards	IEEE 802.3 (10BaseT), IEEE 802.3u (100BaseTX), IEEE 802.11b/g (Wireless)
Operating Range	Wireless - Open space: 100 – 300m; Indoor: 30 - 100m
RF – 802.11g (backwards compatible to 802.11b)	
Frequency Band	2412 ~ 2484 MHz (subject to local regulation)
Modulation Technology	OFDM and DSSS
Modulation Techniques	64QAM, 16QAM, QPSK, BPSK, DBPSK, DQPSK, CCK
Data Rates	54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 Mbps, auto fallback
Output power	18 dBm Peak Power@ Nominal Temp Range
Receive Sensitivity	-70dBm @54Mbps, Nominal Temp Range
Antenna	External Antenna 2dBi
Regulatory and Environmental Compliance	
EMC certification	FCC part 15 (USA)
	CE (Europe)
Temperature Range	Operating: 0 ~ 40 degree C, Storage: -20 ~ 65 degree C
Humidity	10% ~ 85% Non-condensing
Mechanical	
Packaging	Generic, GIGABYTE, private labeling optional
LED indicator	Power/Status LED (Dual Color, Green/Red) Wireless LED (Green) Ethernet Port LED (Green)
Weight	240 ± 5g
Dimensions	110 x 160 x 25 mm

Appendix C: PC Configuration

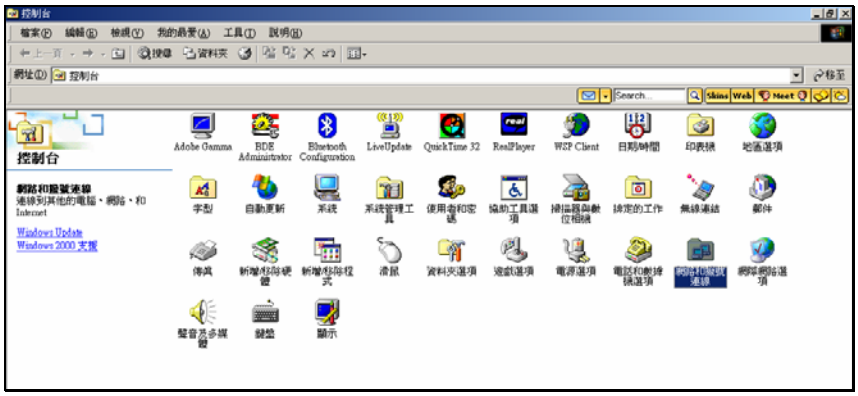
To connect to the AP, your computer needs to be located in the same Subnet as the AP. Please follow the instructions given to setup in a TCP/IP network environment. By default, Windows 98, *Me*, 2000 and XP already have TCP/IP installed. If you have not installed the TCP/IP communication Protocol, please install it now, and then select your operating system for the setup.

TCP/IP Settings Under Windows 2000

Step 1. Click the **Start** button, select **Settings** and then click the **Control Panel** icon.



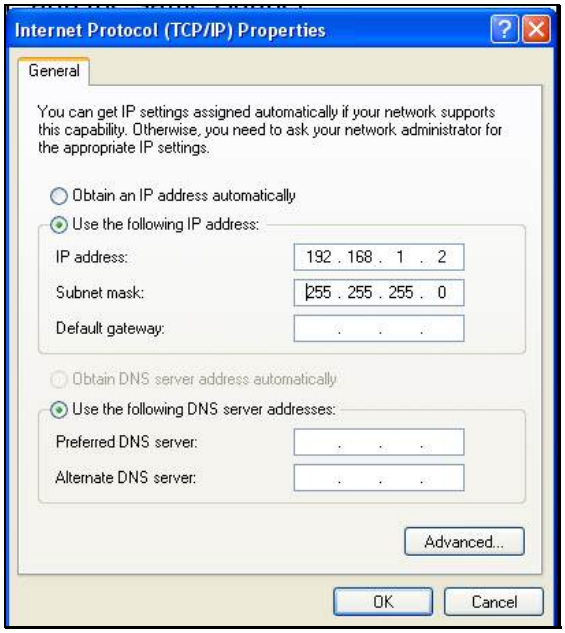
Step 2. Double-click the **Network and Dial-up Connection** icon.



Step 3. Double-click the **"LAN CONNECTION"** and click the **"Properties"** button.

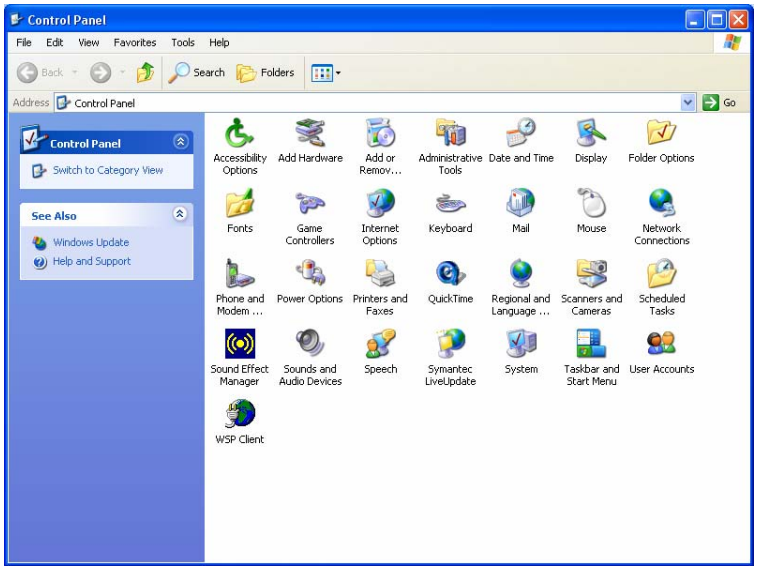
Step 4. The **"Local Area Connection Properties"** dialog box will appear. Verify that the Internet Protocol (TCP/IP) item is checked. Then double-click on **Internet Protocol (TCP/IP)**.

Step 5. Assign the static IP address used by the AP and the same Subnet Mask to the computer (For example, IP address is 192.168.1.2 and Subnet Mask is 255.255.255.0), click the “OK” button to return to Local Area Connection Properties. Click the “OK” button again to complete the PC configuration.

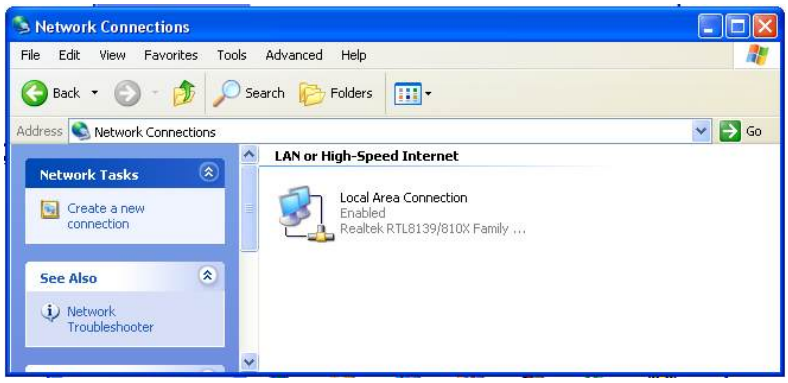

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 2
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

TCP/IP Settings under Windows XP

Step 1. Click the **"Start"** in the desktop of the Windows to select **"Settings"**, and then select the **"Control Panel"**.

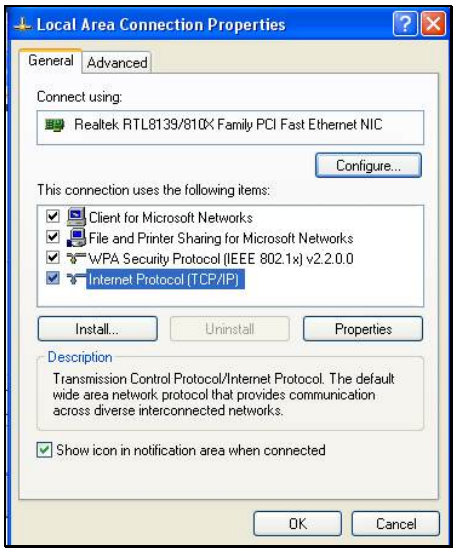


Step 2. Double-click the **"Network Connections"** icon.

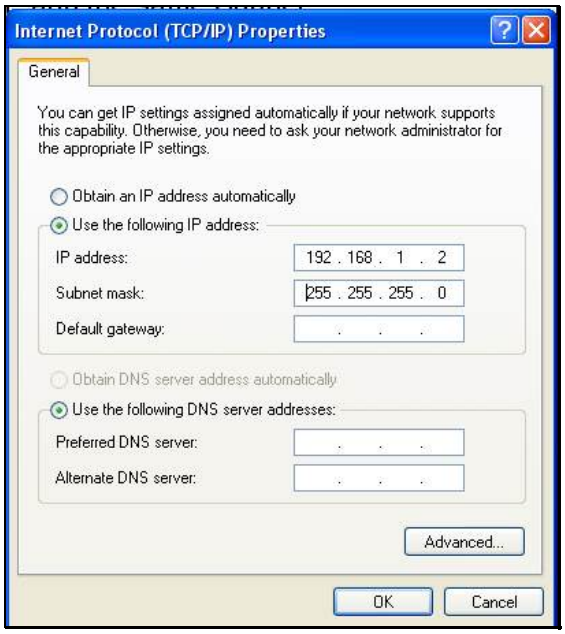


Step 3. Double-click the **"LAN CONNECTION"** and click the **"Properties"** button.

Step 4. The **"Local Area Connection Properties"** dialog box will appear. Verify that the Internet Protocol (TCP/IP) item is checked. And then double-click on **"Internet Protocol (TCP/IP)"** item.



Step 5. Assign the static IP address used by the AP and the same Subnet Mask to the computer (For example, IP address is192.168.1.2 and Subnet Mask is 255.255.255.0), click the “OK” button to return to **“Local Area Connection Properties”**. Click the “OK” button again to complete the PC configuration.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 2
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Appendix D
Warranty

Limited Warranty Statement (1-Year Warranty)

Thank you for purchasing the GIGABYTE Product. This limited warranty statement will provide you one year warranty starting from the purchase date. Of which if any defect is occurred due to accidents or any man-made factors, or any unauthorized torn-off or damage to GIGABYTE's sticker on the product, GIGABYTE Technology will not provide after-sale services, such as:

- Products are damaged due to any violation of instructions on user manual.
- Hardware is damaged due to inappropriate assembling.
- Products are damaged due to the use of illegal accessory.
- Products are damaged due to parts disassembling without authorization.
- Products are damaged due to exceeding environment limits.
- Products are damaged due to unexpected external force.
- Products are damaged due to nature disasters.
- Products are copies or illegally smuggled goods.

PLEASE RECORD THE FOLLOWING INFORMATION REGARDING YOUR WARRANTY

Name of Customer:	
Phone No:	
Address:	
Email:	
Model:	
Serial:	
Date of Purchase:	
Place of Purchase:	
From Whom:	
Distributor:	

Customer Service

GIGA-BYTE TECHNOLOGY CO., LTD.
No.6, Bau Chiang Road, Hsin-Tien,
Taipei Hsien, Taiwan,
Tel: 886-2-89124888 Fax:886-2-89124007
http://www.GIGABYTE.com.tw